HERBERT B. ENDERTON

UNA INTRODUCCIÓN MATEMÁTICA A LA LÓGICA

Segunda Edición

TRADUCCIÓN:
JOSÉ ALFREDO AMOR MONTAÑO



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
MÉXICO, 2004

E5218
QA9
2004

Enderton, Herbert B., Una introducción matemática a la lógica / Herbert B. Enderton; traducción José Alfredo Amor Montaño. - 2a. ed. - México: UNAM, Instituto de Investigaciones Filosóficas, 2004. - 454 p.

ISBN: 970-32-2144-0 Traducción de: A mathematical introduction to logic

1. Lógica simbólica y matemática. I. Amor Montaño, José Alfredo, tr. II. t.

Título original: *A Mathematical Introduction to Logic 2nd edition*

Instituto de Investigaciones Filosóficas
Circuito Mtro. Mario de la Cueva s/n,
Ciudad Universitaria, Coyoacán, 04510, México, D.F.
Tels.: 5622 7437 y 5622 7504; fax: 5665 4991
Correo electrónico: libros@filosoficas.unam.mx
Página web: http://www.filosoficas.unam.mx

1a. edición en castellano: 1987
2a. edición en castellano: 2004

Composición y formación tipográfica: José Alberto Barrañón C.
Corrección de estilo y cuidado de la edición: Laura E. Manríquez

Impreso y hecho en México
ISBN 970-32-2144-0

PREFACIO

Este libro, como la primera edición, presenta los conceptos y los resultados básicos de la lógica: los temas son pruebas, verdad y computabilidad (o calculabilidad). Como en la edición anterior, la forma en que se presentan los contenidos está dirigida al lector que ya posee algunos conocimientos e intereses matemáticos. En esta versión revisada, además de numerosos cambios "locales", hay tres maneras "globales" en las cuales la presentación cambió.

En primer lugar, he intentado hacer que el material sea más *accesible* para el estudiante de licenciatura típico. En el desarrollo principal he tratado de no dar por sentada información ni conocimientos que pudieran no estar al alcance de un estudiante de matemáticas de nivel medio.

En segundo lugar, para el profesor que quiera adaptar el libro a las necesidades de su curso, la organización del contenido se ha hecho más *flexible*. Los pies de página al comienzo de muchas secciones indican rutas opcionales que el profesor —o el lector independiente— podría elegir.

En tercer lugar, la *ciencia de la computación* teórica ha influido en la lógica en los años recientes, y algunas de esas influencias se reflejan en esta edición. Los problemas de computabilidad se toman más en serio. Algunos materiales sobre modelos finitos se han incorporado al texto.

Esta obra pretende servir como libro de texto para un curso introductorio de matemáticas sobre lógica de nivel medio y avanzado de licenciatura. Los objetivos son presentar los conceptos y teoremas importantes de la lógica y explicar su significación y su relación con el resto del trabajo matemático del lector.

Como libro de texto, puede usarse en cursos cuya duración varíe entre un trimestre y un año. En un trimestre generalmente llego hasta el material sobre modelos de teorías de primer orden (sección 6 del capítulo II). El tiempo adicional que ofrece un semestre permitiría dar un vistazo a la indecidibilidad, consultando, por ejemplo, el panorama que se presenta en la sección 0 del capítulo III. En un segundo semestre, el material del capítulo III (sobre indecidibilidad) puede cubrirse más adecuadamente.

El libro está dirigido al lector que no ha estudiado lógica anteriormente, pero que tiene alguna experiencia con el razonamiento matemático. No hay requisitos específicos aparte de la disposición para funcionar en cierto nivel de abstracción y de rigor. Es inevitable usar la teoría de conjuntos básica. En el capítulo cero ofrecemos un resumen conciso de la teoría de conjuntos que se usa a lo largo de la obra. No es conveniente iniciar el libro estudiando este capítulo, pues éste más bien está pensado como referencia para cuando surja la necesidad —si es que surge—. El profesor puede ajustar la cantidad de teoría de conjuntos que va a dar; por ejemplo, es posible evitar los números cardinales por completo (a costa de perder algunos teoremas). El libro contiene algunos ejemplos tomados del álgebra abstracta, pero son sólo ejemplos y no son esenciales a la exposición. Los últimos capítulos (Caps. III y IV) tienden a exigir más del lector que los primeros.

La inducción y la recursión reciben un tratamiento más extenso (en la sección 4 del capítulo I) que lo acostumbrado. Prefiero dar una explicación intuitiva de estos temas en clase y tener una versión precisa en el libro, y no al revés. Al final de casi todas las secciones se incluyen ejercicios. Si el ejercicio lleva un número en negritas, entonces sus resultados se usan en el texto al exponer el tema. Los ejercicios de dificultad excepcional están marcados con un asterisco.

Reconozco con gusto mi deuda con mis maestros, categoría en la que incluyo también a los que han sido mis colegas o mis alumnos. Me agradaría recibir comentarios y correcciones de parte de los usuarios del libro. El sitio web para el libro se encuentra en http://www.math.ucla.edu/~hbe/amil.

INTRODUCCIÓN

La lógica simbólica es un modelo matemático del pensamiento deductivo. Al menos esto fue cierto en un principio, pues, al igual que otras ramas de la matemática, ha crecido más allá de las circunstancias de su nacimiento. La lógica simbólica es un modelo en el mismo sentido en que la teoría moderna de la probabilidad es un modelo para las situaciones en que intervienen el azar y la incertidumbre.

¿Cómo se construye el modelo? Se comienza con un objeto de la vida real; por ejemplo, un avión. Luego se escogen algunos aspectos de este objeto original que se representarán en el modelo, como su forma, y otros que se pasarán por alto, como su tamaño. Entonces se construye un objeto, semejante al original en algunas propiedades —que escogemos como esenciales— y diferente en otras —que consideramos irrelevantes—. El éxito del modelo para cumplir con su propósito dependerá en gran medida de la selección de las propiedades del objeto original que se representan en el modelo.

La lógica es más abstracta que los aviones. Los objetos de la vida real son ciertas deducciones "lógicamente correctas". Por ejemplo:

> Todos los hombres son mortales.
>
> Sócrates es un hombre.
>
> Por lo tanto, Sócrates es mortal.

La validez de inferir la tercera afirmación —la conclusión— de las dos primeras —las premisas— no depende de idiosincrasias particulares de Sócrates. La inferencia está justificada por la forma de las oraciones más que por algún hecho empírico

acerca de la mortalidad. No importa realmente el significado de "mortal"; lo que sí importa aquí es el significado de "todos".

> Los bórgovos están fefos durante el brilgo.
> Ahora es brilgo y esto es un bórgovo.
> Por lo tanto, esto está fefo.

De nuevo podemos reconocer que la tercera afirmación es consecuencia de las dos primeras, aun cuando no tengamos la menor idea de cómo se ve un bórgovo cuando está fefo.

Las deducciones lógicamente correctas tienen más interés del que podrían sugerir los frívolos ejemplos precedentes. De hecho, la matemática axiomática consiste en una gran cantidad de deducciones de este tipo. Así, las deducciones que realizan los matemáticos constituyen objetos de la vida real cuyas propiedades deberán reflejarse en nuestro modelo.

La correctud lógica de estas deducciones se debe a su forma y es independiente de su contenido. Este criterio es vago, pero es justamente este tipo de vaguedad lo que nos induce a recurrir a los modelos matemáticos. Uno de nuestros objetivos principales será dar, dentro del modelo, una versión precisa de este criterio. Las preguntas (acerca de nuestro modelo) que más nos interesarán al principio serán:

1. ¿Qué quiere decir que una afirmación sea "consecuencia lógica" de otras?

2. Si una afirmación es consecuencia lógica de otras, ¿qué métodos de *demostración* pueden ser necesarios para establecer este hecho?

3. ¿Hay una brecha entre lo que podemos *probar* en un sistema axiomático (digamos, para los números naturales) y lo que es *verdadero* acerca de los números naturales?

4. ¿Cuál es la relación entre la lógica y la computabilidad?

En realidad presentaremos dos modelos. El primero —la lógica proposicional— será muy simple y terriblemente inadecuado para modelar deducciones interesantes. Esto se debe a que preserva sólo algunas propiedades rudimentarias de las deducciones de la vida real. El segundo modelo —la lógica de primer

orden— es admirablemente apropiado para modelar las deducciones que se encuentran en las matemáticas. Cuando un matemático afirma que un enunciado particular se sigue de los axiomas de la teoría de conjuntos, quiere decir que su deducción se puede traducir a una en nuestro modelo.

Este énfasis en las matemáticas guió la selección de temas incluidos. Este libro no incursiona en la lógica multivariada, ni en la lógica modal ni en la lógica intuicionista, que representan selecciones diferentes de propiedades de las deducciones de la vida real.

Hasta ahora hemos evitado dar mucha información acerca del modelo de la lógica de primer orden. Como breves indicaciones, daremos ahora algunos ejemplos de la expresividad de su lenguaje formal. Primero consideremos el enunciado castellano que afirma el principio conjuntista de extensionalidad: "Si exactamente las mismas cosas son elementos de un primer objeto así como de un segundo objeto, entonces ambos objetos son el mismo." Esto puede traducirse a nuestro lenguaje de primer orden como

$$\forall x \forall y \, (\forall z \, (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

Como segundo ejemplo, podemos traducir el enunciado bien conocido por los estudiantes de cálculo: "Para todo número positivo ϵ existe un número positivo δ tal que, para toda x cuya distancia a a sea menor que δ, la distancia entre $f(x)$ y b es menor que ε", como

$$\forall \varepsilon \, (\varepsilon > 0 \rightarrow \exists \delta \, (\delta > 0 \wedge \forall x \, (dxa < \delta \rightarrow dfxb < \varepsilon))).$$

Hemos dado algunas pautas acerca de lo que pretendemos hacer en este libro. También deberíamos evitar algunas posibles impresiones falsas diciendo lo que no haremos. Esta obra no se propone enseñar al lector a pensar. La palabra "lógica" se usa a veces para referirse a recetas para pensar, pero nosotros no la usamos así. El lector ya sabe pensar; aquí se le ofrecen algunos conceptos interesantes en los cuales pensar.

CAPÍTULO CERO

ALGUNOS DATOS ÚTILES DE LA TEORÍA DE CONJUNTOS

Daremos por supuesto que el lector ya está familiarizado en mayor o menor medida con los métodos conjuntistas que se usan normalmente. Sin embargo, haremos aquí un breve resumen de algunos datos de la teoría de conjuntos que necesitaremos; esto servirá al menos para establecer nuestra notación. Sugerimos al lector que, en lugar de lanzarse a estudiar este capítulo, simplemente vuelva a él cuando surjan dudas de naturaleza conjuntista en capítulos posteriores. El libro favorito del autor sobre teoría de conjuntos es, desde luego, *Elements of Set Theory* (véase la lista de referencias al final de este libro).

Primero unas palabras acerca de la jerga lingüística. A lo largo del libro utilizaremos una colección de abreviaturas matemáticas estándar. Usaremos "$\dashv$" para denotar el fin de una prueba. Un enunciado "Si..., entonces..." se abreviará algunas veces "... $\Rightarrow$ ...". También tenemos "$\Leftarrow$" para la implicación inversa (para el modo particular en que el término "implicación" se usa en matemáticas). Para "si y sólo si" usaremos la expresión más breve "sii" (esto se ha convertido en parte del lenguaje matemático), así como el símbolo "$\Leftrightarrow$". Para la expresión "por lo tanto" empleamos la abreviatura "$\therefore$".

El recurso notacional que expresa "$x \neq y$" como la negación de "$x = y$" y "$x \notin y$" como la negación de "$x \in y$" lo extenderemos a otros casos. Por ejemplo, en la sección 2 del capítulo I definimos "$\Sigma \models \tau$"; entonces, "$\Sigma \not\models \tau$" denota su negación.

Ahora bien, un *conjunto* es una colección de cosas; éstas se conocen como sus miembros o elementos. Como es costumbre, escribimos "$t \in A$" para decir que t es un elemento de A, y "$t \notin$

A" para decir que t no es un elemento de A. Escribimos "$x = y$" para significar que x y y son el mismo objeto. Es decir, la expresión "x" a la izquierda del signo de igualdad es un nombre para el mismo objeto que nombra la otra expresión "y". Si $A = B$ entonces, para cualquier objeto t, es automáticamente verdadero que $t \in A$ sii $t \in B$. Esto es cierto sencillamente porque A y B son la misma cosa. La recíproca es el principio de extensionalidad: si A y B son conjuntos tales que para todo objeto t,

$$t \in A \quad \text{sii} \quad t \in B,$$

entonces $A = B$. Esto refleja la idea de lo que *es* un conjunto; un conjunto está determinado justamente por sus miembros.

Adjuntar un objeto adicional a un conjunto es una operación muy útil. Para cualquier conjunto A, sea $A\,;t$ el conjunto cuyos elementos son (i) los elementos de A, más (ii) el elemento (nuevo posiblemente) t. El objeto t puede pertenecer o no ya de antemano a A, y tenemos

$$A\,;t = A \cup \{t\}$$

usando la notación que definiremos más tarde, y

$$t \in A \quad \text{sii} \quad A\,;t = A.$$

Un conjunto especial es el conjunto vacío $\emptyset$, el cual carece de elementos. De cualquier otro conjunto se dice que es *no vacío*. Para cualquier objeto x existe el conjunto unitario $\{x\}$, cuyo único elemento es x. En general, para cualquier número finito $x_1, \ldots, x_n$ de objetos, existe el conjunto $\{x_1, \ldots, x_n\}$, cuyos elementos son exactamente estos objetos. Nótese que $\{x, y\} = \{y, x\}$, ya que ambos conjuntos tienen exactamente los mismos elementos: sólo hemos usado distintas expresiones para denotar el conjunto. Si el orden importa, podemos usar pares ordenados (que veremos más adelante).

Abusaremos un poco de esta notación para abarcar algunos casos infinitos sencillos. Por ejemplo, $\{0, 1, 2, \ldots\}$ es el conjunto $\mathbb{N}$ de los números naturales, y $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ es el conjunto $\mathbb{Z}$ de todos los enteros.

Escribimos "$\{x \mid _x_\}$" para denotar el conjunto de todos los objetos x tales que $_x_$. Nos tomaremos libertades considerables con esta notación: por ejemplo, $\{(m, n) \mid m < n \text{ en } \mathbb{N}\}$

es el conjunto de todas las parejas ordenadas de números naturales cuya primera componente es menor que la segunda. Y $\{x \in A \mid _x_\}$ es el conjunto de todos los elementos x de A tales que $_x_$.

Si A es un conjunto tal que todos sus elementos son también elementos de B, entonces A es un *subconjunto* de B, lo cual se abrevia "$A \subseteq B$". Nótese que todo conjunto es subconjunto de sí mismo. Además, $\emptyset$ es un subconjunto de cualquier conjunto. ("$\emptyset \subseteq A$" es "verdadero vacuamente", ya que el trabajo de verificar que cada elemento de $\emptyset$ también pertenece a A consiste en no hacer nada. Desde otro punto de vista, "$A \subseteq B$" puede ser falso únicamente si algún elemento de A no pertenece a B. Si $A = \emptyset$, esto es imposible.) A partir del conjunto A podemos formar un nuevo conjunto, el *conjunto potencia* $\mathcal{P}A$ de A, cuyos elementos son los subconjuntos de A. Así,

$$\mathcal{P}A = \{x \mid x \subseteq A\}.$$

Por ejemplo,

$$\mathcal{P}\emptyset = \{\emptyset\},$$
$$\mathcal{P}\{\emptyset\} = \{\emptyset, \{\emptyset\}\}.$$

La *unión* de A y B, $A \cup B$, es el conjunto de todas las cosas que son elementos de A o de B (o de ambos). Por ejemplo, $A ; t = A \cup \{t\}$. Análogamente, la *intersección* de A y B, $A \cap B$, es el conjunto de todas las cosas que son elementos tanto de A como de B. A y B son *disjuntos* (o ajenos) sii su intersección es vacía (*i.e.*, si no tienen miembros en común). Una colección de conjuntos es *disjunta dos a dos* sii cualesquiera dos miembros de la colección son disjuntos.

Más en general, considérese un conjunto A cuyos elementos son a su vez conjuntos. La unión de A, $\bigcup A$, es el conjunto que se obtiene amalgamando todos los conjuntos que pertenecen a A en uno solo:

$$\bigcup A = \{x \mid x \text{ pertenece a algún elemento de } A\}.$$

De forma similar, para A no vacío,

$$\bigcap A = \{x \mid x \text{ pertenece a todos los elementos de } A\}.$$

Por ejemplo, si

$$A = \{\{0, 1, 5\}, \{1, 6\}, \{1, 5\}\},$$

entonces

$$\bigcup A = \{0, 1, 5, 6\},$$
$$\bigcap A = \{1\}.$$

Dos ejemplos más:

$$A \cup B = \bigcup \{A, B\},$$
$$\bigcup \mathcal{P}A = A.$$

En los casos en que para cada número natural n tengamos un conjunto A_n, la unión de todos estos conjuntos, $\bigcup\{A_n \mid n \in \mathbb{N}\}$, se suele denotar mediante "$\bigcup_{n \in \mathbb{N}} A_n$", o simplemente "$\bigcup_n A_n$".

La pareja ordenada $\langle x, y\rangle$ de los objetos x y y debe ser definida de tal manera que

$$\langle x, y\rangle = \langle u, v\rangle \quad \text{sii} \quad x = u \text{ y } y = v.$$

Cualquier definición que tenga esta propiedad servirá; la definición usual es

$$\langle x, y\rangle = \{\{x\}, \{x, y\}\}.$$

Las ternas ordenadas se definen como

$$\langle x, y, z\rangle = \langle\langle x, y\rangle, z\rangle.$$

En general definimos las n-adas recursivamente haciendo

$$\langle x_1, \ldots, x_{n+1}\rangle = \langle\langle x_1, \ldots, x_n\rangle, x_{n+1}\rangle$$

para $n > 1$. Es conveniente definir también $\langle x\rangle = x$; así, la ecuación anterior también se cumple para $n = 1$. S es una *sucesión finita* (o *cadena*) de elementos de A sii existe un entero positivo n tal que $S = \langle x_1, \ldots, x_n\rangle$, donde cada $x_i \in A$. (Las sucesiones finitas a menudo se definen como ciertas funciones finitas, pero la definición anterior es ligeramente más conveniente para nosotros.)

Un *segmento* de la sucesión finita $S = \langle x_1, \ldots, x_n \rangle$ es una sucesión finita

$$\langle x_k, x_{k+1}, \ldots, x_{m-1}, x_m \rangle, \qquad \text{donde} \quad 1 \leq k \leq m \leq n.$$

Este segmento es un *segmento inicial* sii $k = 1$, y es *propio* sii es diferente de S.

Si $\langle x_1, \ldots, x_n \rangle = \langle y_1, \ldots, y_n \rangle$, es fácil probar que $x_i = y_i$ para $1 \leq i \leq n$. (La prueba usa inducción sobre n y la propiedad básica de las parejas ordenadas.) Pero si $\langle x_1, \ldots, x_m \rangle = \langle y_1, \ldots, y_n \rangle$, entonces no se sigue en general que $m = n$. Después de todo, las ternas ordenadas son también parejas ordenadas. Pero afirmamos que m y n pueden ser distintos sólo si alguna x_i es ella misma una sucesión finita de y_j's, o viceversa:

Lema 0A Supongamos que $\langle x_1, \ldots, x_m \rangle = \langle y_1, \ldots, y_m, \ldots, y_{m+k} \rangle$. Entonces $x_1 = \langle y_1, \ldots, y_{k+1} \rangle$.

Demostración Por inducción sobre m. Si $m = 1$, la conclusión es inmediata. Para el paso inductivo, supongamos que $\langle x_1, \ldots, x_m, x_{m+1} \rangle = \langle y_1, \ldots, y_{m+k}, y_{m+1+k} \rangle$. Entonces las primeras componentes de esta pareja ordenada deben ser iguales: $\langle x_1, \ldots, x_m \rangle = \langle y_1, \ldots, y_{m+k} \rangle$. Aplíquese ahora la hipótesis inductiva. ⊣

Por ejemplo, supongamos que A es un conjunto tal que ningún elemento de A es una sucesión finita de otros elementos. Entonces si $\langle x_1, \ldots, x_m \rangle = \langle y_1, \ldots, y_n \rangle$ y cada x_i y y_j están en A, entonces, por el lema anterior, $m = n$. Por lo cual tenemos también que $x_i = y_i$.

A partir de los conjuntos A y B podemos formar su *producto cartesiano*: el conjunto $A \times B$ de todas las parejas $\langle x, y \rangle$ tales que $x \in A$ y $y \in B$. A^n es el conjunto de todas las n-adas de elementos de A. Por ejemplo, $A^3 = (A \times A) \times A$.

Una relación R es un conjunto de parejas ordenadas. Por ejemplo, la relación de orden para los números 0–3 es capturada por —y de hecho *es igual a*— el conjunto de las parejas ordenadas

$$\{\langle 0, 1 \rangle, \langle 0, 2 \rangle, \langle 0, 3 \rangle, \langle 1, 2 \rangle, \langle 1, 3 \rangle, \langle 2, 3 \rangle\}.$$

El *dominio* de R (que se escribe dom R) es el conjunto de todos los objetos x tales que $\langle x, y \rangle \in R$ para alguna y. El *rango* (o

imagen) de R (que se escribe ran R) es el conjunto de todos los objetos y tales que $\langle x, y\rangle \in R$ para alguna x. La unión de dom R y ran R es el *campo* de R, cam R.

Una *relación n-aria* en A es un subconjunto de A^n. Si $n > 1$, hay una relación. Pero una relación 1-*aria* (unaria) en A es simplemente un subconjunto de A. Una relación binaria particularmente sencilla en A es la relación de igualdad $\{\langle x,x\rangle \mid x \in A\}$ en A. Si R es una relación n-aria en A, y B es un subconjunto de A, la *restricción* de R a B es la intersección $R \cap B^n$. Por ejemplo, la relación mostrada anteriormente es la restricción al conjunto $B = \{0, 1, 2, 3\}$ de la relación de orden sobre $\mathbb{N}$.

Una *función* es una relación F que tiene la propiedad de ser *de un solo valor*: para cada x en dom F existe una única y tal que $\langle x, y\rangle \in F$. Como es costumbre, llamamos a esta única y el valor $F(x)$ que toma F en x. (Esta notación data de Euler. Es una lástima que no haya elegido $(x)F$ en lugar de $F(x)$, lo que habría sido de ayuda para la *composición* de funciones: $f \circ g$ es la función cuyo valor en x es $f(g(x))$, que se obtiene al aplicar primero g y después f.)

Decimos que *F es una función de A en B* y escribimos

$$F : A \to B$$

para significar que F es una función, dom $F = A$ y ran $F \subseteq B$. Si además ran $F = B$, entonces F es una función de A *sobre* B, F es *uno a uno* sii para cada y en ran F existe una única x tal que $\langle x, y\rangle \in F$. Si la pareja $\langle x, y\rangle$ pertenece a dom F, escribimos $F(x, y) = F(\langle x, y\rangle)$. Esta notación se extiende a las n-adas: $F(x_1, \ldots, x_n) = F(\langle x_1, \ldots, x_n\rangle)$.

Una *operación n-aria* en A es una función de A^n en A. Por ejemplo, la suma es una operación binaria en $\mathbb{N}$, mientras que la operación *sucesor*, S (donde $S(n) = n + 1$), es una operación unaria en $\mathbb{N}$. Si f es una operación n-aria en A, la *restricción* de f a un subconjunto B de A es la función g con dominio B^n que coincide con f en cada punto de B^n. Así,

$$g = f \cap (B^n \times A).$$

Esta g será una operación n-aria en B sii B está *cerrado* bajo f, en el sentido de que $f(b_1, \ldots, b_n) \in B$ siempre que cada b_i esté

en B. En este caso, $g = f \cap B^{n+1}$, de acuerdo con la forma en que hemos definido la restricción de una relación. Por ejemplo, la operación suma en $\mathbb{N}$, la cual contiene ternas tales como $\langle\langle 3, 2\rangle, 5\rangle$, es la restricción a $\mathbb{N}$ de la operación suma en $\mathbb{R}$, la cual contiene muchas más ternas.

Una operación unaria particularmente sencilla en A es la función *identidad* Id en A, dada por la ecuación

$$Id(x) = x \qquad \text{para} \quad x \in A.$$

Así, $Id = \{\langle x, x\rangle \mid x \in A\}$.

Para una relación R tenemos las siguientes definiciones:

R es *reflexiva* en A sii $\langle x, x\rangle \in R$ para toda x en A.

R es *simétrica* sii siempre que $\langle x, y\rangle \in R$, entonces también $\langle y, x\rangle \in R$.

R es *transitiva* sii siempre que $\langle x, y\rangle \in R$ y $\langle y, z\rangle \in R$ (si esto sucediera), entonces también $\langle x, z\rangle \in R$.

R satisface la *tricotomía* en A sii para cualesquiera x y y en A, se cumple exactamente una de las siguientes tres posibilidades: $\langle x, y\rangle \in R$, o $x = y$, o $\langle y, x\rangle \in R$.

R es una *relación de equivalencia* en A sii R es una relación binaria en A que es reflexiva en A, simétrica y transitiva.

R es una *relación de orden* en A sii R es transitiva y satisface la tricotomía en A.

Si R es una relación de equivalencia en A definimos, para cada $x \in A$, la *clase de equivalencia* $[x]$ de x como $\{y \mid \langle x, y\rangle \in R\}$. Las clases de equivalencia forman entonces una *partición* de A. Esto es, las clases de equivalencia son subconjuntos de A tales que todo elemento de A pertenece exactamente a una clase de equivalencia. Si x y y pertenecen a A,

$$[x] = [y] \quad \text{sii} \quad \langle x, y\rangle \in R.$$

El conjunto $\mathbb{N}$ de los números naturales es el conjunto $\{0, 1, 2, \ldots\}$. (Los números naturales también se pueden definir conjuntistamente, un punto que se toca brevemente en la sección 7 del capítulo III.) Un conjunto A es *finito* sii hay alguna función uno a uno f de A sobre $\{0, 1, \ldots, n-1\}$ (para

algún número natural n). (Podemos pensar que f "cuenta" los elementos de A.)

Un conjunto A es *numerable* sii existe alguna función uno a uno de A en $\mathbb{N}$. Por ejemplo, todo conjunto finito es evidentemente numerable. Ahora consideremos un conjunto infinito numerable A. Entonces, a partir de la función uno a uno dada f de A en $\mathbb{N}$, podemos extraer una función uno a uno f' de A *sobre* $\mathbb{N}$. Para alguna $a_0 \in A$, $f(a_0)$ es el mínimo elemento de ran f; sea $f'(a_0) = 0$. En general existe una única $a_n \in A$ tal que $f(a_n)$ es el $(n+1)$-ésimo elemento de ran f; sea $f'(a_n) = n$. Nótese que $A = \{a_0, a_1, \ldots\}$. (También podemos pensar que f' "cuenta" los elementos de A, sólo que ahora el proceso de conteo es infinito.)

Teorema 0B Sea A un conjunto numerable. Entonces el conjunto de las sucesiones finitas de elementos de A también es numerable.

Demostración El conjunto S de todas las sucesiones finitas en A se puede caracterizar mediante la ecuación

$$S = \bigcup_{n \in \mathbb{N}} A^{n+1}.$$

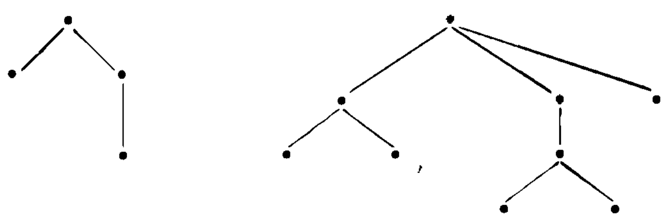
Como A es numerable, existe una función uno a uno f de A en $\mathbb{N}$.

La idea básica es construir la función uno a uno de S en $\mathbb{N}$ asignando a $\langle a_0, a_1, \ldots, a_m \rangle$ el número $2^{f(a_0)+1} 3^{f(a_1)+1} \cdot \ldots \cdot p_m^{f(a_m)+1}$, donde p_m es el $(m+1)$-ésimo primo. Esto tiene el defecto de que tal asignación pudiera no estar bien definida, ya que podría suceder que $\langle a_0, a_1, \ldots, a_m \rangle = \langle b_0, b_1, \ldots, b_n \rangle$, con a_i y b_j en A pero con $m \neq n$. No obstante, esto no representa un problema serio; se resuelve asignando a cada elemento de S el *mínimo* número que se puede obtener de la manera anterior. Así obtenemos una función bien definida; es fácil ver que es uno a uno. ⊣

En algunas partes hablaremos de *árboles*, los cuales pueden ser útiles para tener imágenes intuitivas de algunas situaciones.

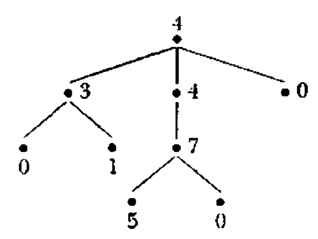
Pero nuestros comentarios sobre árboles siempre serán informales, ya que excluimos este concepto de los teoremas y de sus demostraciones. En consecuencia, nuestra discusión aquí acerca de los árboles será informal.

Para cada árbol existe un orden parcial finito subyacente. Podemos dibujar una figura de este orden parcial R; si $\langle a, b \rangle \in R$, entonces colocamos a debajo de b y conectamos los puntos con una línea. Dos figuras típicas de órdenes correspondientes a árboles son las siguientes:



(En matemáticas, los árboles crecen hacia abajo, no hacia arriba.) Siempre hay un punto hasta arriba de la figura (la *raíz*). Además, si bien se permite la ramificación por debajo de un vértice, los puntos *por encima* de cualquier vértice dado deben quedar todos sobre la misma línea.

Además de este orden parcial finito subyacente, un árbol también tiene una función que etiqueta los vértices. Por ejemplo, el siguiente es un árbol en el que las etiquetas son números naturales:



En algunos pasajes del libro usaremos el axioma de elección; pero casi todos estos usos se pueden eliminar si los teoremas en cuestión se restringen a lenguajes numerables. De los muchos

enunciados equivalentes al axioma de elección, el lema de Zorn es especialmente útil.

Una colección C de conjuntos es una *cadena* sii para cualesquiera elementos x y y de C, $x \subseteq y$ o $y \subseteq x$.

> **Lema de Zorn** Sea A un conjunto tal que para toda cadena $C \subseteq A$, el conjunto $\bigcup C$ pertenece a A. Entonces existe algún elemento $m \in A$ que es maximal en el sentido de que no es subconjunto de ningún otro elemento de A.

Números cardinales

Todos los conjuntos infinitos son grandes, pero algunos son más grandes que otros. (Por ejemplo, el conjunto de los números reales es más grande que el conjunto de los enteros.) Los números cardinales ofrecen una forma conveniente, aunque no indispensable, de hablar acerca del tamaño de los conjuntos.

Es natural decir que dos conjuntos A y B tienen el mismo tamaño sii existe una función uno a uno de A sobre B. Si A y B son finitos, este concepto es equivalente al usual: si se cuentan los elementos de A y los de B, se obtiene el mismo número en ambas ocasiones. Pero el concepto se aplica incluso a conjuntos infinitos A y B, en los cuales es difícil contar.

Formalmente, entonces, A y B son *equipotentes* (se escribe: $A \sim B$) sii existe una función uno a uno de A sobre B. Por ejemplo, el conjunto $\mathbb{N}$ de los números naturales y el conjunto $\mathbb{Z}$ de los enteros son equipotentes. Es fácil ver que la equipotencia es reflexiva, simétrica y transitiva.

Para los conjuntos finitos podemos usar los números naturales como medidas del tamaño. El mismo número natural se asignaría a dos conjuntos finitos (como medida de su tamaño) sii los conjuntos son equipotentes. Los números cardinales se introducen para permitirnos generalizar esta situación a los conjuntos infinitos.

A cada conjunto A le podemos asignar cierto objeto, el *número cardinal* (o *cardinalidad*) de A (se escribe: card A), de tal manera que a dos conjuntos se les asigne la misma cardinalidad sii son equipotentes

$$\operatorname{card} A = \operatorname{card} B \quad \text{sii} \quad A \sim B. \tag{K}$$

Hay varias maneras de lograr esto; la usual hoy en día es hacer card A igual al mínimo ordinal equipotente a A. (El éxito de esta definición depende del axioma de elección.) No discutiremos los ordinales aquí, ya que para nuestros propósitos no tiene mucha importancia saber qué es realmente card A, así como tampoco tiene importancia saber realmente qué es el número 2. Lo más importante es que (K) se cumple. Es conveniente, sin embargo, que si A es un conjunto finito, card A sea el número natural que diga cuántos elementos tiene A. Algo es un *número cardinal* (o simplemente un *cardinal*) sii es card A para algún conjunto A.

(Georg Cantor, quien introdujo por primera vez el concepto de número cardinal, caracterizó en 1895 el número cardinal de un conjunto M como "el concepto general que, con ayuda de nuestra inteligencia activa, surge del conjunto M por la abstracción de la naturaleza de sus varios elementos y del orden en que están dados".)

Decimos que A está *dominado* por B ($A \preceq B$) sii A es equipotente a algún subconjunto de B. En otras palabras, $A \preceq B$ sii existe una función uno a uno de A en B. El concepto correspondiente para cardinales es

$$\operatorname{card} A \leq \operatorname{card} B \quad \text{sii} \quad A \preceq B.$$

(Es fácil ver que $\leq$ está bien definido; esto es, que $\kappa \leq \lambda$ depende solamente de los cardinales κ y λ, no de una elección particular de dos conjuntos con tales cardinalidades.) La dominancia es reflexiva y transitiva. Un conjunto A está dominado por $\mathbb{N}$ sii A es numerable. El siguiente es un resultado estándar en este tema.

Teorema de Schröder-Bernstein (a) Si A y B son conjuntos tales que $A \preceq B$ y $B \preceq A$, entonces $A \sim B$.
(b) Si κ y λ son cardinales tales que $\kappa \leq \lambda$ y $\lambda \leq \kappa$, entonces $\kappa = \lambda$.

La parte (b) es una simple reformulación de la parte (a) en términos de números cardinales. El siguiente teorema, que por cierto es equivalente al axioma de elección, está enunciado de la misma manera dual.

Teorema 0C (a) Si A y B son conjuntos cualesquiera, entonces $A \preceq B$ o $B \preceq A$.
(b) Si κ y λ son cardinales cualesquiera, entonces $\kappa \leq \lambda$ o $\lambda \leq \kappa$.

Así, dados dos números cardinales, uno es menor que el otro. (De hecho, todo conjunto no vacío de números cardinales contiene un mínimo elemento.) Los cardinales más pequeños son los de los conjuntos finitos: 0, 1, 2, ... Luego está el mínimo cardinal infinito, card $\mathbb{N}$, que recibe el nombre de $\aleph_0$. De esta manera tenemos

$$0, 1, 2, \ldots, \aleph_0, \aleph_1, \ldots,$$

donde $\aleph_1$ es el mínimo cardinal mayor que $\aleph_0$. La cardinalidad del conjunto $\mathbb{R}$, de los números reales, se llama "$2^{\aleph_0}$". Como $\mathbb{R}$ no es numerable, $\aleph_0 < 2^{\aleph_0}$.

Las operaciones de suma y multiplicación, ya bien conocidas para los cardinales finitos, se pueden extender a todos los cardinales. Para calcular $\kappa + \lambda$ elegimos conjuntos disjuntos A y B de cardinalidades κ y λ, respectivamente. Entonces

$$\kappa + \lambda = \text{card}(A \cup B).$$

Esto está bien definido; es decir, $\kappa + \lambda$ depende solamente de κ y λ y no de la elección de los conjuntos disjuntos A y B. Definimos la multiplicación como

$$\kappa \cdot \lambda = \text{card}(A \times B).$$

Está claro que estas definiciones son correctas para cardinales finitos. La aritmética de los cardinales infinitos es sorprendentemente sencilla (con el axioma de elección). La suma o producto de dos cardinales infinitos es simplemente el mayor de ellos:

Teorema de aritmética cardinal Si κ y λ son cardinales tales que $\kappa \leq \lambda$ y λ es infinito, entonces $\kappa + \lambda = \lambda$. Además, si $\kappa \neq 0$, entonces $\kappa \cdot \lambda = \lambda$.

En particular, si κ es un cardinal infinito,

$$\aleph_0 \cdot \kappa = \kappa.$$

Teorema 0D Si A es un conjunto infinito, el conjunto $\bigcup_n A^{n+1}$ de todas las sucesiones finitas de elementos de A tiene cardinalidad igual a card$A$.

Ya hemos probado esto para el caso en que A es numerable (véase el teorema 0B).

Demostración Cada A^{n+1} tiene cardinalidad igual a card$A$, por el teorema sobre la aritmética cardinal (aplicado n veces). Entonces tenemos la unión de $\aleph_0$ conjuntos de este tamaño, lo que da por resultado $\aleph_0 \cdot \text{card}\, A = \text{card}\, A$ puntos en total. ⊣

Ejemplo Del teorema anterior se sigue que el conjunto de los números algebraicos tiene cardinalidad $\aleph_0$. Primero, podemos identificar cada polinomio (en una variable) sobre los enteros, con la sucesión de sus coeficientes. Luego, por el teorema hay $\aleph_0$ polinomios. Cada polinomio tiene un número finito de raíces. Para dar una cota superior extravagante, nótese que aun si cada polinomio tuviera $\aleph_0$ raíces, tendríamos entonces $\aleph_0 \cdot \aleph_0 = \aleph_0$ números algebraicos en total. Como al menos hay $\aleph_0$, ya no tenemos más que demostrar.

Como hay una cantidad no numerable (de hecho, $2^{\aleph_0}$) de números reales, se sigue que hay una cantidad no numerable (de hecho, $2^{\aleph_0}$) de números trascendentes.

I

LÓGICA DE ENUNCIADOS

0. *Observaciones informales sobre los lenguajes formales*

En la siguiente sección construiremos un lenguaje al cual podremos traducir oraciones del español. A diferencia de los lenguajes naturales (como el español o el chino), éste será un lenguaje formal, con reglas de formación precisas. Pero antes de que comience la precisión, discutiremos aquí algunas de las características que deseamos incorporar a este lenguaje.

Como primer ejemplo, el enunciado "Se observaron rastros de potasio" se puede traducir al lenguaje formal usando, digamos, el símbolo **K**. Entonces para el enunciado relacionado "No se observaron rastros de potasio", podemos usar $(\neg \mathbf{K})$. Aquí $\neg$ es nuestro símbolo para la negación, que se lee "no". También se podría pensar en traducir "No se observaron rastros de potasio" usando un nuevo símbolo, por ejemplo, **J**, pero preferiremos descomponer los enunciados como éste en partes atómicas hasta donde sea posible. Para un enunciado que no está relacionado, "La muestra contenía cloro", elegimos, digamos, el símbolo **C**. Luego las fórmulas de la derecha son posibles traducciones de los siguientes enunciados compuestos:

Si se observaron rastros de potasio, entonces la muestra no contenía cloro.	$(\mathbf{K} \rightarrow (\neg \mathbf{C}))$
La muestra contenía cloro y se observaron rastros de potasio.	$(\mathbf{C} \wedge \mathbf{K})$

En el segundo enunciado usamos el símbolo de conjunción $\wedge$ como traducción de "y". El primero utiliza la flecha, que

es más conocida, como traducción de "si. . ., entonces. . ." En el siguiente ejemplo usamos el símbolo de disyunción $\vee$ para traducir "o":

No se observaron rastros de potasio, o la muestra no contenía cloro.	$((\neg \mathbf{K}) \vee (\neg \mathbf{C}))$
Ni la muestra contenía cloro, ni se observaron rastros de potasio:	$(\neg(\mathbf{C} \vee \mathbf{K}))$ o bien $((\neg \mathbf{C}) \wedge (\neg \mathbf{K}))$

En este último enunciado hemos dado dos traducciones alternativas. La relación que guardan entre sí se discutirá más adelante.

Un aspecto importante de las descomposiciones que haremos de los enunciados compuestos es que siempre que se nos den la verdad o la falsedad de las partes atómicas, podremos entonces calcular inmediatamente la verdad o la falsedad del compuesto. Supongamos, por ejemplo, que el químico sale de su laboratorio y anuncia que observó rastros de potasio, pero que la muestra no contenía cloro. Sabremos luego que los cuatro enunciados anteriores son verdadero, falso, verdadero y falso, respectivamente. De hecho, podemos construir de antemano una tabla con los cuatro resultados experimentales posibles (Tabla I). Reanudaremos la discusión de dichas tablas en la sección 2 de este capítulo.

Tabla I

$\mathbf{K}$	$\mathbf{C}$	$(\neg(\mathbf{C} \vee \mathbf{K}))$	$((\neg \mathbf{C}) \wedge (\neg \mathbf{K}))$
F	*F*	*V*	*V*
F	*V*	*F*	*F*
V	*F*	*F*	*F*
V	*V*	*F*	*F*

El uso de lenguajes formales nos permitirá escapar de la imprecisión y las ambigüedades de los lenguajes naturales; sin embargo, esto tiene su precio: nuestros lenguajes formales tendrán un grado de expresividad muy limitado.

La descripción de un lenguaje formal incluirá generalmente tres tipos de datos:

1. Especificaremos el conjunto de símbolos (el alfabeto). En el caso presente, la lógica de enunciados, algunos de los símbolos son

$$(,), \rightarrow, \neg, A_1, A_2, \ldots$$

2. Especificaremos las reglas para formar las sucesiones finitas de símbolos "gramaticalmente correctas". (Tales sucesiones se denominarán *fórmulas*.) Por ejemplo, en este caso,

$$(A_1 \rightarrow (\neg A_2))$$

será una fórmula, mientras que

$$)) \rightarrow A_3$$

no lo será.

3. También indicaremos las traducciones permisibles entre el español y el lenguaje formal. Los símbolos $A_1, A_2, \ldots$ pueden ser traducciones de enunciados declarativos del español.

Sólo en esta tercera parte daremos a las fórmulas algún significado. Este proceso de asignación de significado guía y motiva todo lo que hacemos; pero también podrá notarse que, teóricamente, sería posible realizar varias manipulaciones de las fórmulas en absoluta ignorancia de cualquier significado posible. Una persona que estuviera al tanto sólo de las dos primeras partes de la información podría realizar algunas de las cosas que haremos, pero esto no tendría ningún sentido para ella.

Antes de proceder, examinemos brevemente otra clase de lenguajes formales de interés generalizado hoy en día; se trata de los lenguajes usados por las computadoras digitales (o que al menos están en conexión con ellas).

Existen muchos de estos lenguajes; en uno de ellos una fórmula típica es

011010110101000111100010000011111010.

En otro, una fórmula típica es

STEP#ADDIMAX, A.

(Aquí # es un símbolo llamado espacio; se incluye en el alfabeto para que toda fórmula sea una cadena de símbolos.) Un lenguaje muy conocido llamado C++ tiene fórmulas como la siguiente:

while(*s ++);

En todos los casos hay un procedimiento para traducir las fórmulas al español y (para una clase restringida de oraciones del español) un procedimiento para traducir del español al lenguaje formal. No obstante, la computadora ignora la lengua castellana; la computadora, un autómata no pensante, manipula símbolos y obedece ciegamente a su programa. Nosotros también podríamos estudiar los lenguajes formales de esa manera, pero no sería tan divertido.

1. *El lenguaje de la lógica de enunciados*

Supondremos que se nos da una sucesión infinita de objetos distintos a los que llamaremos símbolos y a los cuales ahora daremos nombre (Tabla II). Supondremos, además, que ninguno de estos símbolos es una sucesión finita de otros símbolos.

Ahora resultan pertinentes varias observaciones:

1. Los cinco símbolos

$$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$$

se llaman *conectivos de enunciado*; su uso se sugiere en la traducción dada en la tabla II. Los conectivos, junto con los paréntesis, son los *símbolos lógicos*. Al traducirlos del español y al español siempre desempeñan el mismo papel. Los símbolos de enunciado son los *parámetros* (o *símbolos no lógicos*). Su traducción no está fija; más bien estarán abiertos a una gran diversidad de interpretaciones, como pronto mostraremos.

2. Hemos incluido una cantidad infinita de símbolos de enunciado. Por una parte, una alternativa más modesta sería tener *un* símbolo de enunciado A y una prima $'$. Entonces podríamos usar la sucesión potencialmente infinita

$$A, A', A'', \ldots$$

Tabla II

Símbolo	Nombre largo	Observaciones
(	paréntesis izquierdo	puntuación
)	paréntesis derecho	puntuación
$\neg$	símbolo de negación	español: no
$\wedge$	símbolo de conjunción	español: y
$\vee$	símbolo de disyunción	español: o (inclusivo)
$\rightarrow$	símbolo de condicional	español: si __, entonces __
$\leftrightarrow$	símbolo de bicondicional	español: si y sólo si
A_1	primer símbolo de enunciado	
A_2	segundo símbolo de enunciado	
...		
A_n	enésimo símbolo de enunciado	
...		

en lugar de

$$A_1, A_2, A_3, \ldots$$

Esta alternativa tiene la ventaja de que disminuye a nueve el número total de símbolos diferentes. Por otra parte, una alternativa *menos* modesta sería permitir un conjunto arbitrario de símbolos de enunciado, numerable o no. La mayor parte de las cosas que se digan en este capítulo seguirían siendo aplicables en este caso: las excepciones se encuentran principalmente en la sección 7 de este capítulo.

3. Algunos lógicos prefieren llamar a A_n el *enésimo símbolo de proposición* (y hablan de lógica proposicional en vez de llamarla lógica de enunciados). Esto se debe a que desean que la palabra "enunciado" haga referencia a un caso particular de oración y que una proposición sea lo que un enunciado afirma.

4. Llamamos "símbolos" a estos objetos, pero nos mantenemos neutrales acerca de cuál pudiera ser su estatus ontológico. En la columna de la extrema izquierda de nuestra lista de símbolos (tabla II) están sus nombres; por ejemplo, A_{243} es un

símbolo, a saber, el bicentésimo cuadragésimo tercer símbolo de enunciado. (Por otra parte, A_{243} es un nombre para ese símbolo. El símbolo condicional puede o no tener la propiedad geométrica de estar conformado como una flecha, aunque su nombre "$\rightarrow$" sí la tiene.) Los símbolos pueden ser conjuntos, números, canicas u objetos pertenecientes a un universo de objetos lingüísticos. En este último caso, es concebible que sean de hecho las mismas cosas que los nombres que usamos para ellos. Otra posibilidad, que explicaremos en el siguiente capítulo, es que los símbolos de enunciados sean fórmulas de otro lenguaje.

5. Hemos supuesto que ningún símbolo es una sucesión finita de otros símbolos. Con esto queremos decir que los símbolos de la lista no sólo son distintos (*v.gr.*: $A_3 \neq \leftrightarrow$), sino que, además, ninguno de ellos es una sucesión finita de dos o más símbolos. Por ejemplo, exigimos que $A_3 \neq \langle \neg, A_4, (\rangle$. El propósito de esta suposición es asegurar que las sucesiones finitas de símbolos tengan una descomposición única. En otras palabras, si

$$\langle a_1, \ldots, a_m \rangle = \langle b_1, \ldots, b_n \rangle$$

y cada a_i y cada b_j es un símbolo, entonces $m = n$ y $a_i = b_i$. (Véase el capítulo cero, lema 0A, y las observaciones subsiguientes.)

Una *expresión* es una sucesión finita de símbolos. Podemos especificar una expresión concatenando los nombres de los símbolos; así $(\neg A_1)$ es la sucesión $\langle (, \neg, A_1,) \rangle$. Esta notación se extiende: si α y β son sucesiones de símbolos, entonces $\alpha\beta$ es la sucesión que consiste en los símbolos de la sucesión α seguidos de los símbolos de la sucesión β.

Por ejemplo, si α y β son las expresiones dadas por las ecuaciones

$$\alpha = (\neg A_1),$$
$$\beta = A_2,$$

entonces $(\alpha \rightarrow \beta)$ es la expresión

$$((\neg A_1) \rightarrow A_2).$$

Ahora debemos examinar algunos ejemplos de posibles traducciones de enunciados del español a expresiones del lengua-

je formal. Sean **A**, **B**, . . . , **Z** los primeros 26 símbolos de enunciado. (Por ejemplo, $\mathbf{E} = \mathbf{A}_5$.)

1. Español: El sospechoso debe ser liberado. Traducción: **R**.

Español: La evidencia obtenida es admisible. Traducción: **E**.

Español: La evidencia obtenida es inadmisible. Traducción: $(\neg \mathbf{E})$.

Español: La evidencia obtenida es admisible y el sospechoso no debe ser liberado. Traducción: $(\mathbf{E} \wedge (\neg \mathbf{R}))$.

Español: La evidencia obtenida es admisible o el sospechoso debe ser liberado (o posiblemente ambas cosas). Traducción: $(\mathbf{E} \vee \mathbf{R})$.

Español: O bien la evidencia obtenida es admisible, o bien el sospechoso debe ser liberado, pero no ambas cosas. Traducción: $((\mathbf{E} \vee \mathbf{R}) \wedge (\neg (\mathbf{E} \wedge \mathbf{R})))$. Siempre usaremos el símbolo $\vee$ como traducción de la palabra "o" en su sentido inclusivo "y/o".

Español: La evidencia obtenida es inadmisible, pero el sospechoso no debe ser liberado. Traducción: $((\neg \mathbf{E}) \wedge (\neg \mathbf{R}))$. Por otra parte, la expresión $((\neg \mathbf{E}) \vee (\neg \mathbf{R}))$ se traduce al español como: La evidencia obtenida es inadmisible, o el sospechoso no debe ser liberado.

2. Español: Si mi abuela tiene ruedas, es bicicleta. Traducción: $(\mathbf{R} \rightarrow \mathbf{B})$.

Español: Mi abuela es bicicleta si y sólo si tiene ruedas. Traducción: $(\mathbf{R} \leftrightarrow \mathbf{B})$.

3. Español: Este artículo constituye riqueza si y sólo si es transferible, de abastecimiento limitado, y produce placer o evita dolor. Traducción: $(\mathbf{R} \leftrightarrow (\mathbf{T} \wedge (\mathbf{L} \wedge (\mathbf{P} \vee \mathbf{Q}))))$. Aquí, **R** es la traducción de "Este artículo constituye riqueza". Por supuesto que en el ejemplo anterior usamos **R** para traducir un enunciado distinto. No estamos atados a una sola traducción.

Advertencia: No se debe confundir un enunciado del español (Las rosas son rojas) con una traducción de dicho enunciado al lenguaje formal (*v.gr.*, **R**); son diferentes. Es de suponer que el enunciado en español es verdadero o falso; pero la expresión formal es sólo una sucesión de símbolos. Desde luego, se puede interpretar en algún contexto como un enunciado verdadero (o

falso) del español, pero puede tener otras interpretaciones en otros contextos.

Ahora bien, algunas expresiones no se pueden obtener como traducciones de ningún enunciado castellano y no son más que disparates; por ejemplo,

$$((\rightarrow \mathbf{A}_3.$$

Queremos definir las fórmulas como expresiones "gramaticalmente correctas"; las expresiones sin sentido habrán de ser excluidas. La definición tendrá las siguientes consecuencias:

(a) Todo símbolo de enunciado es una fórmula.

(b) Si α y β son fórmulas, entonces también lo son $(\neg\alpha)$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$ y $(\alpha \leftrightarrow \beta)$.

(c) Ninguna expresión es una fórmula a menos que (a) y (b) obliguen a ello.

Queremos hacer más precisa esta tercera propiedad (acerca de la obligatoriedad). Una fórmula es una expresión que puede construirse a partir de símbolos de enunciado aplicando un número finito de veces las *operaciones de construcción de fórmulas* (en las expresiones) definidas por las ecuaciones

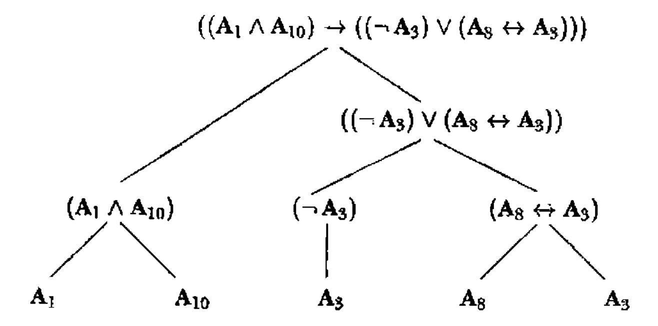
$$\begin{aligned}
\mathcal{E}_{\neg}(\alpha) &= (\neg\alpha),\\
\mathcal{E}_{\wedge}(\alpha,\beta) &= (\alpha \wedge \beta),\\
\mathcal{E}_{\vee}(\alpha,\beta) &= (\alpha \vee \beta),\\
\mathcal{E}_{\rightarrow}(\alpha,\beta) &= (\alpha \rightarrow \beta),\\
\mathcal{E}_{\leftrightarrow}(\alpha,\beta) &= (\alpha \leftrightarrow \beta).
\end{aligned}$$

Por ejemplo,

$$((\mathbf{A}_1 \wedge \mathbf{A}_{10}) \rightarrow ((\neg\mathbf{A}_3) \vee (\mathbf{A}_8 \leftrightarrow \mathbf{A}_3)))$$

es una fórmula, como se puede ver si examinamos su árbol genealógico (p. 35).

El árbol ilustra cómo se construye la expresión a partir de cuatro símbolos de enunciado y aplicando cinco veces operaciones de construcción de fórmulas. Este ejemplo es atípico



por el hecho de que usa todas las operaciones de construcción de fórmulas. Veamos un ejemplo menor: A_3 es una fórmula; su árbol genealógico tiene sólo un vértice aislado; cada operación de construcción de fórmulas se aplica cero veces. Pero este caso es demasiado pequeño; no consideraremos que la sucesión vacía se ha "construido a partir de los símbolos de enunciado".

Esta clase de construcción, que consiste en tomar algunos bloques constructivos básicos (aquí, los símbolos de enunciado) y "cerrar" bajo algunas operaciones (aquí, cinco operaciones), ocurre frecuentemente en lógica y en otras ramas de las matemáticas. En la sección 4 de este capítulo examinaremos esta clase de construcciones en un marco más general.

Podemos desarrollar la idea de "construcción" como sigue. Definamos una *sucesión de construcción* como una sucesión finita $\langle \varepsilon_1, \ldots, \varepsilon_n \rangle$ de expresiones tal que, para cada $i \leq n$, tenemos al menos uno de los siguientes hechos:

ε_i es un símbolo de enunciado
$\varepsilon_i = \mathcal{E}_\neg(\varepsilon_j)$ para algún $j < i$
$\varepsilon_i = \mathcal{E}_\square(\varepsilon_j, \varepsilon_k)$ para algunos $j < i$, $k < i$

donde $\square$ es uno de los conectivos binarios, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$. Entonces las fórmulas pueden caracterizarse como las expresiones α tales que alguna sucesión de construcción termina con α. Podemos concebir ε_i como la expresión en el estado i del proceso de construcción.

Para nuestro primer ejemplo

$$((\mathbf{A}_1 \wedge \mathbf{A}_{10}) \rightarrow ((\neg \mathbf{A}_3) \vee (\mathbf{A}_8 \leftrightarrow \mathbf{A}_3)))$$

obtenemos una sucesión de construcción al comprimir su árbol genealógico en un orden lineal.

Una característica de esta clase de construcción es que genera un *principio de inducción*. Decimos que un conjunto S es *cerrado* bajo una función f de dos argumentos sii cada vez que $x \in S$ y $y \in S$, entonces $f(x, y) \in S$, y análogamente para funciones de un argumento, etcétera.

Principio de inducción Si S es un conjunto de fórmulas que contiene todos los símbolos de enunciado y es cerrado bajo las cinco operaciones de construcción de fórmulas, entonces S es el conjunto de *todas* las fórmulas.

Primera demostración Considérese una fórmula α arbitraria. Entonces α está construida a partir de símbolos de enunciado al aplicar un número finito de veces las operaciones de construcción de fórmulas. Explorando hacia arriba el árbol genealógico correspondiente, encontraremos que cada expresión que hay en el árbol pertenece a S. A la larga (o sea, después de un número finito de pasos), en la punta del árbol encontraremos que $\alpha \in S$. ⊣

Segunda demostración Repetiremos el argumento, pero sin árboles. Considérese una fórmula α arbitraria. Entonces α es el último miembro de alguna sucesión de construcción $\langle \varepsilon_1, \ldots, \varepsilon_n \rangle$. Por inducción numérica fuerte ordinaria sobre el número i, veremos que cada $\varepsilon_i \in S$, $i \leq n$.

Es decir, suponemos, como nuestra hipótesis inductiva, que $\varepsilon_j \in S$ para toda $j < i$. Luego verificamos que $\varepsilon_i \in S$, considerando los diferentes casos. Así, por inducción fuerte sobre i, se sigue que $\varepsilon_i \in S$ para cada $i \leq n$. En particular, el último miembro α pertenece a S. ⊣

Usaremos ampliamente este principio en las páginas que siguen; en el ejemplo que aparece a continuación lo emplearemos para probar que ciertas expresiones *no* son fórmulas.

EJEMPLO Ninguna expresión con más paréntesis izquierdos que paréntesis derechos es una fórmula.

Demostración La idea es que al construir una fórmula comenzamos con símbolos de enunciado (que tienen cero paréntesis izquierdos y cero paréntesis derechos), y luego aplicamos las operaciones de construcción de fórmulas, cada una de las cuales agrega paréntesis sólo por parejas, uno izquierdo y otro derecho. El argumento se puede reformular como sigue: El conjunto de las fórmulas "balanceadas" (las que tienen igual número de paréntesis izquierdos que derechos) tiene como elementos a todos los símbolos de enunciado y es cerrado bajo las operaciones de construcción de fórmulas. Es decir, el conjunto de las fórmulas balanceadas es inductivo. El principio de inducción nos asegura, entonces, que todas las fórmulas son balanceadas. ⊣

Una característica especial de nuestras operaciones de construcción de fórmulas particulares es que construyen *hacia arriba* y nunca *hacia abajo*. Esto es, las expresiones $\mathcal{E}_{\square}(\alpha, \beta)$ siempre incluyen como segmento la sucesión completa α (y la sucesión completa β) además de otros símbolos. En particular, es más larga que α o que β.

Esta característica especial simplificará el problema de determinar, dada una fórmula φ, *cómo* fue construida exactamente. Todos los bloques de construcción, por decirlo así, están incluidos como segmentos en la sucesión φ. Por ejemplo, si φ no contiene el símbolo $\mathbf{A}_4$, entonces φ puede construirse sin usar nunca $\mathbf{A}_4$. (Véase el ejercicio 4.)

Ejercicios

1. Escriba tres enunciados en español junto con sus traducciones a nuestro lenguaje formal. Los enunciados se deberán escoger de manera que tengan una estructura interesante, y cada traducción deberá contener quince o más símbolos.

2. Muestre que no hay fórmulas de longitud 2, 3 ni 6, pero que cualquier otra longitud es posible.

3. Sea α una fórmula; sea c el número posible de lugares en los que aparecen símbolos de conectivo binarios ($\wedge$,

$\vee, \rightarrow, \leftrightarrow$) en α; sea s el número de lugares en los que aparecen símbolos de enunciado en α. (Por ejemplo, si α es $(\mathbf{A} \rightarrow (\neg \mathbf{A}))$, entonces $c = 1$ y $s = 2$.) Usando el principio de inducción, pruebe que $s = c + 1$.

4. Suponga que tenemos una sucesión de construcción que termina en φ, donde φ no contiene el símbolo $\mathbf{A}_4$. Suponga que en la sucesión de construcción borramos todas las expresiones que contienen $\mathbf{A}_4$. Muestre que el resultado es todavía una sucesión de construcción correcta.

5. Suponga que α es una fórmula que no contiene el símbolo de negación $\neg$.

   (a) Muestre que la longitud de α (es decir, el número de símbolos en la sucesión) es impar.

   (b) Muestre que más de una cuarta parte de los símbolos son símbolos de enunciado.

   Sugerencia: Aplique inducción para mostrar que la longitud es de la forma $4k + 1$ y el número de símbolos de enunciado es $k + 1$.

2. *Asignaciones de verdad*

Queremos definir lo que significa que una fórmula de nuestro lenguaje se siga lógicamente de otras fórmulas. Por ejemplo, $\mathbf{A}_1$ deberá seguirse de $(\mathbf{A}_1 \wedge \mathbf{A}_2)$, pues independientemente de cómo se traduzcan los parámetros $\mathbf{A}_1$ y $\mathbf{A}_2$ al español, si la traducción de $(\mathbf{A}_1 \wedge \mathbf{A}_2)$ es verdadera, entonces la traducción de $\mathbf{A}_1$ debe ser verdadera. Pero la noción de todas las posibles traducciones al español es demasiado vaga. Afortunadamente, el espíritu de esta noción puede expresarse de una manera simple y precisa.

Fijemos de una vez por todas un conjunto $\{F, V\}$ de *valores de verdad* consistente en dos puntos distintos:

F, llamado *falsedad*,
V, llamado *verdad*.

(Lo que estos puntos son en sí mismos carece de importancia; bien podrían ser los números 0 y 1.) Entonces una *asignación de*

verdad v para un conjunto S de símbolos de enunciado es una función

$$v : S \to \{F, V\}$$

que asigna V o F a cada símbolo de S. Estas asignaciones de verdad serán usadas en lugar de las traducciones al español mencionadas en el párrafo precedente.

(En este momento nos hemos comprometido a usar la lógica *bivalente*. También es posible estudiar la lógica trivalente, en cuyo caso tenemos un conjunto de tres posibles valores de verdad. Y luego, por supuesto, sólo hay un pequeño paso adicional para permitir 512 o $\aleph_0$ valores de verdad, o tomar como conjunto de valores de verdad el intervalo $[0, 1]$ o algún otro espacio conveniente. Un caso particularmente interesante es aquel en el que los valores de verdad forman un álgebra booleana completa. Pero es la lógica bivalente la que siempre ha tenido la mayor importancia, y nos restringiremos a ella.)

Sea $\overline{S}$ el conjunto de fórmulas que pueden construirse a partir de S con las cinco operaciones de construcción de fórmulas. ($\overline{S}$ también puede caracterizarse como el conjunto de fórmulas cuyos símbolos de enunciado pertenecen a S; véanse las observaciones al final de la sección precedente.) Queremos una extensión $\overline{v}$ de v,

$$\overline{v} : \overline{S} \to \{F, V\},$$

que asigne el valor correcto de verdad a cada fórmula de $\overline{S}$. Deberá satisfacer las siguientes condiciones:

0. Para cualquier $A \in S$, $\overline{v}(A) = v(A)$. (Así, $\overline{v}$ es una extensión de v.)

Para cualesquiera α, β en $\overline{S}$:

1. $\overline{v}((\neg \alpha)) = \begin{cases} V & \text{si } \overline{v}(\alpha) = F, \\ F & \text{en los demás casos.} \end{cases}$

2. $\overline{v}((\alpha \land \beta)) = \begin{cases} V & \text{si } \overline{v}(\alpha) = V \text{ y } \overline{v}(\beta) = V, \\ F & \text{en los demás casos.} \end{cases}$

3. $\overline{v}((\alpha \lor \beta)) = \begin{cases} V & \text{si } \overline{v}(\alpha) = V \text{ o } \overline{v}(\beta) = V \text{ (o ambos)}, \\ F & \text{en el otro caso.} \end{cases}$

4. $\overline{v}((\alpha \to \beta)) = \begin{cases} F & \text{si } \overline{v}(\alpha) = V \text{ y } \overline{v}(\beta) = F \\ V & \text{en los demás casos.} \end{cases}$

5. $\overline{v}((\alpha \leftrightarrow \beta)) = \begin{cases} V & \text{si } \overline{v}(\alpha) = \overline{v}(\beta), \\ F & \text{en los demás casos.} \end{cases}$

En la tabla III aparecen las condiciones 1-5 en forma sinóptica. Es aquí donde entra, en nuestros procedimientos formales, el significado que queremos que tenga, por ejemplo, el símbolo de conjunción. Nótese especialmente el significado de $\to$. Siempre que a α se le asigna el valor de F, entonces $(\alpha \to \beta)$ se considera "verdadera por vacuidad" y se le asigna el valor V. Para éste y otros conectivos, desde luego es posible preguntar hasta qué punto hemos reflejado adecuadamente el significado común en el habla cotidiana de "si. . ., entonces", "o", etc. Pero en última instancia nos preocupan más los enunciados matemáticos que los matices sutiles del habla cotidiana.

Tabla III

α	β	$\neg(\alpha)$	$(\alpha \wedge \beta)$	$(\alpha \vee \beta)$	$(\alpha \to \beta)$	$(\alpha \leftrightarrow \beta)$
V	V	F	V	V	V	V
V	F	F	F	V	F	F
F	V	V	F	V	V	F
F	F	V	F	F	V	V

Por ejemplo, podríamos traducir el enunciado en español "Si usted está diciendo la verdad, entonces yo soy el tío de un mono", por la fórmula $(\mathbf{V} \to \mathbf{M})$. Asignamos a esta fórmula el valor V siempre que usted diga mentiras. Al asignar el valor V, ciertamente no estamos afirmando ninguna conexión causal entre su veracidad y alguna característica simiesca de mis sobrinos o sobrinas. El enunciado en cuestión es una afirmación *condicional*. Hace una aseveración acerca de mis parientes siempre que se cumpla cierta *condición* —que usted esté diciendo la verdad—. Cuando esa condición no se cumple, la afirmación es vacuamente verdadera.

De modo muy general, podemos pensar que una fórmula condicional $(\alpha \to \beta)$ expresa la *promesa* de que si cierta con-

dición se cumple (a saber, que α sea verdadera), entonces β es verdadera. Si resulta que la condición α no se cumple, entonces la promesa no se ha roto, independientemente de β.

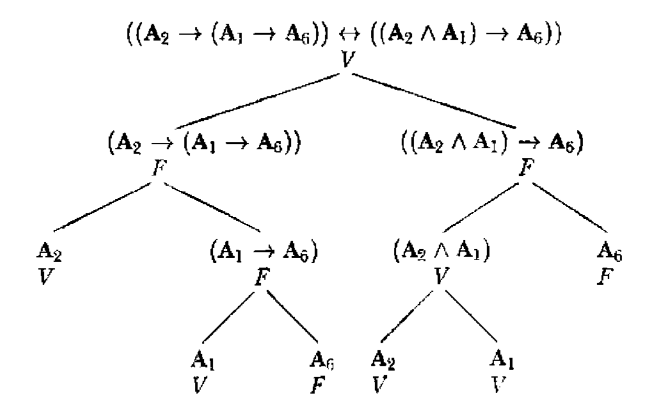
Como ejemplo de la forma de calcular $\overline{v}$, sea la fórmula

$$((\mathbf{A}_2 \rightarrow (\mathbf{A}_1 \rightarrow \mathbf{A}_6)) \leftrightarrow ((\mathbf{A}_2 \wedge \mathbf{A}_1) \rightarrow \mathbf{A}_6))$$

y sea v la asignación de verdad para $\{\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_6\}$ tal que

$$v(\mathbf{A}_1) = V,$$
$$v(\mathbf{A}_2) = V,$$
$$v(\mathbf{A}_6) = F.$$

Queremos calcular $\overline{v}(\alpha)$. Podemos examinar el árbol que muestra la construcción de α:

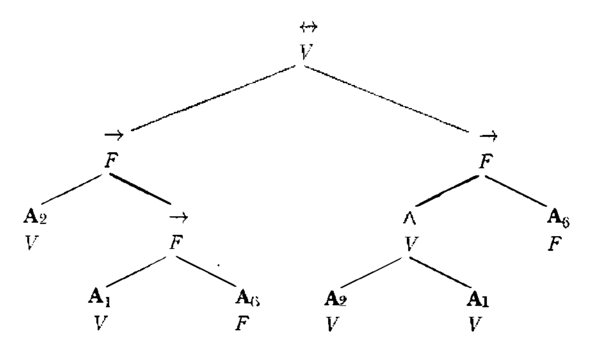


Desplazándonos de abajo hacia arriba, podemos asignar a cada vértice β del árbol el valor $\overline{v}(\beta)$. De modo que, como primer paso, calculamos

$$\overline{v}((\mathbf{A}_1 \rightarrow \mathbf{A}_6)) = F \qquad \text{y} \qquad \overline{v}((\mathbf{A}_2 \wedge \mathbf{A}_1)) = V.$$

Luego calculamos $\overline{v}((\mathbf{A}_2 \rightarrow (\mathbf{A}_1 \rightarrow \mathbf{A}_6))) = F$, y así sucesivamente. Finalmente, en el vértice superior del árbol llegamos a $\overline{v}(\alpha) = V$.

De hecho, este cálculo se puede realizar escribiendo mucho menos. En primer lugar, el árbol se puede representar de manera más concisa:



Y aun esto puede comprimirse en una sola línea (usando de nuevo los paréntesis):

$$\begin{array}{l}((\mathbf{A}_2 \rightarrow (\mathbf{A}_1 \rightarrow \mathbf{A}_6)) \leftrightarrow ((\mathbf{A}_2 \wedge \mathbf{A}_1) \rightarrow \mathbf{A}_6)).\\ \quad V \;\; F \;\; V \;\; F \; F \quad\; V \quad\;\; V \; V V \quad\; F \; F\end{array}$$

Teorema 12A Si v es una asignación de verdad para el conjunto S, entonces existe una única función $\overline{v} : \overline{S} \rightarrow \{F, V\}$ que satisface las condiciones 0–5 que mencionamos páginas antes.

La demostración completa de este teorema surgirá en las siguientes dos secciones (3 y 4); pero ya debería parecer sumamente plausible, en especial a la luz del ejemplo anterior. Al demostrar la existencia de $\overline{v}$, el punto crucial será, esencialmente, la unicidad de los árboles mencionados en el ejemplo.

Decimos que una asignación de verdad v *satisface* φ sii $\overline{v}(\varphi) = V$. (Por supuesto, para que esto ocurra, todos los símbolos de enunciado de φ deben pertenecer al dominio de v.) Ahora consideremos un conjunto Σ de fórmulas (que desempeñan el papel de hipótesis) y otra fórmula τ (que desempeña el de posible conclusión).

Definición Σ *implica tautológicamente* τ (que se escribe: $\Sigma \models \tau$) sii toda asignación de verdad para los símbolos de

enunciado que ocurren en Σ y en τ, que satisface todos los elementos de Σ también satisface τ.

Esta definición refleja nuestra idea intuitiva de que una conclusión se sigue de un conjunto de hipótesis si la suposición de que las hipótesis son verdaderas garantiza la verdad de la conclusión.

Varios casos especiales del concepto de implicación tautológica merecen ser mencionados. Primero tomemos el caso especial en el que Σ es el conjunto vacío $\emptyset$. Obsérvese que es cierto por vacuidad que toda asignación de verdad satisface todos los elementos de $\emptyset$. (¿Cómo podría fallar esto? Sólo si existiera algún elemento no satisfecho de $\emptyset$, lo cual es absurdo.) Por tanto, tenemos: $\emptyset \models \tau$ sii toda asignación de verdad (para los símbolos de enunciado que aparecen en τ) satisface τ. En este caso decimos que τ es una *tautología* (lo que se escribe: $\models \tau$). En un ejemplo anterior encontramos que la fórmula $((\mathbf{A}_2 \rightarrow (\mathbf{A}_1 \rightarrow \mathbf{A}_6)) \leftrightarrow ((\mathbf{A}_2 \wedge \mathbf{A}_1) \rightarrow \mathbf{A}_6))$ es satisfecha por una de las ocho posibles asignaciones de verdad para $\{\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_6\}$. De hecho, las otras siete asignaciones también satisfacen esta fórmula, la cual, por tanto, es una tautología.

Otro caso especial es aquel en que ninguna asignación de verdad satisface todos los elementos de Σ. Entonces, para toda τ es cierto por vacuidad que $\Sigma \models \tau$. Por ejemplo,

$$\{\mathbf{A}, (\neg\mathbf{A})\} \models \mathbf{B}.$$

Lo anterior no involucra ningún principio profundo, es sólo un producto secundario de nuestras definiciones.

Ejemplo $\{\mathbf{A}, (\mathbf{A} \rightarrow \mathbf{B})\} \models \mathbf{B}$. Hay cuatro posibles asignaciones de verdad para $\{\mathbf{A}, \mathbf{B}\}$. Es fácil verificar que sólo una de estas cuatro satisface tanto $\mathbf{A}$ como $(\mathbf{A} \rightarrow \mathbf{B})$, a saber, la v para la cual $v(\mathbf{A}) = v(\mathbf{B}) = V$. Esta v también satisface B.

Si Σ es el conjunto unitario $\{\sigma\}$ de la fórmula σ, entonces escribimos "$\sigma \models \tau$" en lugar de "$\{\sigma\} \models \tau$". Si a la vez $\sigma \models \tau$ y $\tau \models \sigma$, entonces se dice que σ y τ son *tautológicamente equivalentes* (que se escribe: $\sigma \models\!\dashv \tau$). Por ejemplo, en la sección cero de este capítulo encontramos las fórmulas $(\neg(\mathbf{C} \vee \mathbf{K}))$ y

$((\neg \mathbf{C}) \wedge (\neg \mathbf{K}))$ como traducciones alternativas de una oración castellana. Ahora podemos afirmar que son tautológicamente equivalentes.

Podemos enunciar aquí un hecho no trivial que probaremos más adelante (en la sección 7).

> **Teorema de compacidad** Sea Σ un conjunto infinito de fórmulas tal que para todo subconjunto finito Σ_0 de Σ existe una asignación de verdad que satisface todos los elementos de Σ_0. Entonces existe una asignación de verdad que satisface todos los elementos de Σ.

Este teorema se puede reformular de manera más sencilla: Si todo subconjunto finito de Σ es satisfactible, entonces Σ es satisfactible. (El lector familiarizado con algo de topología general podría intentar descubrir por qué este teorema se llama "de compacidad"; el teorema afirma la compacidad de cierto espacio topológico. Luego el lector podría probar el teorema usando el teorema de Tychonoff sobre productos topológicos.)

Tablas de verdad

Hay un procedimiento sistemático, que ahora ilustraremos, para verificar, dadas las fórmulas $\sigma_1, \ldots, \sigma_k$, y τ, si

$$\{\sigma_1, \ldots, \sigma_k\} \models \tau$$

o no. En particular (cuando $k = 0$), el procedimiento decidirá, dada una fórmula, si ésta es una tautología o no.

Como primer ejemplo, podemos probar que

$$(\neg (\mathbf{A} \wedge \mathbf{B})) \models ((\neg \mathbf{A}) \vee (\neg \mathbf{B})).$$

Para hacer esto, consideremos todas las asignaciones de verdad para $\{\mathbf{A}, \mathbf{B}\}$. Hay cuatro asignaciones; en general hay 2^n asignaciones de verdad para un conjunto de n símbolos de enunciado. Las cuatro se pueden escribir en una tabla:

A	**B**
V	*V*
V	*F*
F	*V*
F	*F*

Esta tabla se puede extender entonces para que incluya $(\neg (\mathbf{A} \wedge \mathbf{B}))$ y $((\neg \mathbf{A}) \vee (\neg \mathbf{B}))$. Para cada fórmula calculamos las *V* y las *F* de la manera antes descrita, y se escribe el valor de verdad debajo del conectivo correcto (Tabla IV). (Las dos columnas de la izquierda en la tabla IV son en realidad innecesarias.) A partir de esta tabla ahora podemos ver que todas aquellas asignaciones de verdad que satisfacen $(\neg (\mathbf{A} \wedge \mathbf{B}))$, y que son tres, también satisfacen $((\neg \mathbf{A}) \vee (\neg \mathbf{B}))$.

Tabla IV

A	B	$(\neg (\mathbf{A} \wedge \mathbf{B}))$	$((\neg \mathbf{A}) \vee (\neg \mathbf{B}))$
V	*V*	*F V V V*	*F V F F V*
V	*F*	*V V F F*	*F V V V F*
F	*V*	*V F F V*	*V F V F V*
F	*F*	*V F F F*	*V F V V F*

De hecho, la inversa también es cierta y, por tanto,

$$(\neg(\mathbf{A} \wedge \mathbf{B})) \models\!\dashv ((\neg \mathbf{A}) \vee (\neg \mathbf{B})).$$

Para probar que $(\neg (\mathbf{A} \wedge \mathbf{B})) \not\models ((\neg \mathbf{A}) \wedge (\neg \mathbf{B}))$, podemos construir la tabla de la misma manera. Sin embargo, sólo es necesaria una línea de la tabla para establecer que realmente existe una asignación de verdad que satisface $(\neg (\mathbf{A} \wedge \mathbf{B}))$ y que no satisface $((\neg \mathbf{A}) \wedge (\neg \mathbf{B}))$.

Es probable que cuanto más general sea la aplicabilidad de un procedimiento, menor sea su eficiencia. Por ejemplo, para mostrar que

$$\models ((\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C})) \leftrightarrow ((\mathbf{A} \vee \mathbf{B}) \wedge (\mathbf{A} \vee \mathbf{C}))),$$

podríamos aplicar el método de tablas de verdad; pero esto requiere ocho renglones (correspondientes a ocho posibles asignaciones de verdad para $\{\mathbf{A}, \mathbf{B}, \mathbf{C}\}$). Con un poco de ingenio se puede hacer menos tedioso:

((A	∨	(B	∧	C))	↔	((A	∨	B)	∧	(A	∨	C))).
V	*V*				*V*	*V*	*V*		*V*	*V*	*V*	
F	*F*	*F*	*F*		*V*	*F*	*F*	*F*	*F*	*F*		
F	*V*	*V*	*V*	*V*	*V*	*F*	*V*	*V*	*V*	*F*	*V*	*V*

En el primer renglón supusimos solamente que $v(\mathbf{A}) = V$. Como esta información es suficiente para obtener V para la fórmula, suponemos en todos los demás renglones que $v(\mathbf{A}) = F$. En el segundo renglón suponemos que $v(\mathbf{B}) = F$; esto de nuevo nos permite obtener V para la fórmula. De modo que podemos restringirnos al caso en que $v(\mathbf{B}) = V$. Como la expresión es simétrica en **B** y **C**, también podemos suponer que $v(\mathbf{C}) = V$. Esto nos deja sólo con el tercer renglón, con el que hemos terminado.

Como ejemplo de la manera de evadir una tabla de dieciséis renglones, considérese la siguiente tautología:

(((($\mathbf{P}$	$\wedge$	$\mathbf{Q}$)	$\to$	$\mathbf{R}$)	$\to$	$\mathbf{S}$)	$\to$	(($\mathbf{P}$	$\to$	$\mathbf{R}$)	$\to$	$\mathbf{S}$)).
							V				V	V
	F		V		F	F	V					
V	V	V	R	R	$\overline{R}$	F	V	V	R	R	$\overline{R}$	F

En el primer renglón nos deshacemos del caso en que $v(\mathbf{S}) = V$. En el segundo nos deshacemos del caso en que $v(\mathbf{P}) = F$ o $v(\mathbf{Q}) = F$. El tercer renglón incorpora las dos posibilidades restantes; aquí R es el valor de verdad asignado a **R** y $\overline{R}$ es el valor opuesto.

En el ejemplo anterior es posible ver directamente por qué es una tautología: mientras más fuerte sea el antecedente (la expresión del lado izquierdo), más débil será el condicional. Así,

$$(\mathbf{P} \wedge \mathbf{Q}) \models \mathbf{P},$$
$$(\mathbf{P} \to \mathbf{R}) \models ((\mathbf{P} \wedge \mathbf{Q}) \to \mathbf{R}),$$
$$(((\mathbf{P} \wedge \mathbf{Q}) \to \mathbf{R}) \to \mathbf{S}) \models ((\mathbf{P} \to \mathbf{R}) \to \mathbf{S}).$$

El problema de desarrollar procedimientos efectivos que reduzcan el trabajo tedioso es importante para la demostración de teoremas por computadora. Quizá algunos de los programas requieran examinar fórmulas de la lógica de enunciados con miles de símbolos de enunciado. Las tablas de verdad son demasiado largas para cualquier caso de esta magnitud. El problema del desarrollo de métodos altamente eficientes es un área actual de investigación en la ciencia de la computación.

Digresión. Aplicar el método de tablas de verdad —desarrollado completamente— a una fórmula con n símbolos de enunciado requiere hacer una tabla de 2^n renglones. El problema es

que, conforme n aumenta, 2^n crece "exponencialmente". Por ejemplo, supongamos que usted puede generar la tabla a razón de un millón de renglones por segundo. (Estamos suponiendo, desde luego, que se ayuda de una computadora.) Entonces, si $n = 80$, digamos, usted necesitará "tan sólo" 2^{80} microsegundos para hacer la tabla completa. ¿Cuánto tiempo es eso? Convertidos en años, 2^{80} microsegundos son alrededor de 38 mil millones de años. Como comparación, la edad del universo es de alrededor de quince mil millones de años. La conclusión es que 2^{80} microsegundos ¡es más tiempo del que ha transcurrido hasta hoy!

¿Existe un método más rápido? ¿Podría haber algún método general que, dada cualquier fórmula α con n símbolos de enunciado, determine si α es o no una tautología en sólo $10n^5$ microsegundos (o alguna otra función de n que crezca como un polinomio en lugar de crecer exponencialmente)? (Para $n = 80$, $10n^5$ microsegundos se convierte sólo en nueve horas.) No se conoce la respuesta a esta pregunta, pero la creencia más extendida es que es negativa. Este problema se denomina "P contra NP", y es el problema sin resolver más famoso en la ciencia de la computación teórica de hoy.

Algunas tautologías selectas

1. Leyes asociativas y conmutativas para $\wedge$, $\vee$, $\leftrightarrow$.
2. Leyes distributivas:

$$((\mathbf{A} \wedge (\mathbf{B} \vee \mathbf{C})) \leftrightarrow ((\mathbf{A} \wedge \mathbf{B}) \vee (\mathbf{A} \wedge \mathbf{C}))).$$
$$((\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C})) \leftrightarrow ((\mathbf{A} \vee \mathbf{B}) \wedge (\mathbf{A} \vee \mathbf{C}))).$$

3. Negación:

$$((\neg (\neg \mathbf{A})) \leftrightarrow \mathbf{A}).$$
$$((\neg (\mathbf{A} \to \mathbf{B})) \leftrightarrow (\mathbf{A} \wedge (\neg \mathbf{B}))).$$
$$((\neg (\mathbf{A} \leftrightarrow \mathbf{B})) \leftrightarrow ((\mathbf{A} \wedge (\neg \mathbf{B})) \vee ((\neg \mathbf{A}) \wedge \mathbf{B}))).$$

Leyes de De Morgan:

$$((\neg (\mathbf{A} \wedge \mathbf{B})) \leftrightarrow ((\neg \mathbf{A}) \vee (\neg \mathbf{B}))).$$
$$((\neg (\mathbf{A} \vee \mathbf{B})) \leftrightarrow ((\neg \mathbf{A}) \wedge (\neg \mathbf{B}))).$$

4. Otras:

Tercero excluido:	$(\mathbf{A} \vee (\neg \mathbf{A}))$.
Contradicción:	$(\neg(\mathbf{A} \wedge (\neg \mathbf{A})))$.
Contraposición:	$((\mathbf{A} \to \mathbf{B}) \leftrightarrow ((\neg \mathbf{B}) \to (\neg \mathbf{A})))$.
Exportación:	$(((\mathbf{A} \wedge \mathbf{B}) \to \mathbf{C}) \leftrightarrow (\mathbf{A} \to (\mathbf{B} \to \mathbf{C})))$.

Ejercicios

1. Pruebe que ninguna de las siguientes dos fórmulas implica tautológicamente a la otra:

$$(\mathbf{A} \leftrightarrow (\mathbf{B} \leftrightarrow \mathbf{C})),$$
$$((\mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C})) \vee ((\neg \mathbf{A}) \wedge ((\neg \mathbf{B}) \wedge (\neg \mathbf{C})))).$$

   Sugerencia: Sólo se necesitan dos asignaciones de verdad, no ocho.

2. (a) ¿Es $(((\mathbf{P} \to \mathbf{Q}) \to \mathbf{P}) \to \mathbf{P})$ una tautología?

   (b) Defina σ_k recursivamente como sigue: $\sigma_0 = (\mathbf{P} \to \mathbf{Q})$ y $\sigma_{k+1} = (\sigma_k \to \mathbf{P})$. ¿Para cuáles valores de k es σ_k una tautología? (La parte (a) corresponde a $k = 2$.)

3. (a) Determine si $((\mathbf{P} \to \mathbf{Q}) \vee (\mathbf{Q} \to \mathbf{P}))$ es una tautología o no.

   (b) Determine si $((\mathbf{P} \wedge \mathbf{Q}) \to \mathbf{R})$ implica tautológicamente $((\mathbf{P} \to \mathbf{R}) \vee (\mathbf{Q} \to \mathbf{R}))$, o no.

4. Pruebe que se cumple lo siguiente:

   (a) $\Sigma; \alpha \models \beta$ sii $\Sigma \models (\alpha \to \beta)$.

   (b) $\alpha \models\!\!\!\dashv \beta$ sii $\models (\alpha \leftrightarrow \beta)$.

   (Recuerde que $\Sigma; \alpha = \Sigma \cup \{\alpha\}$, el conjunto Σ junto con el posiblemente nuevo elemento α.)

5. Pruebe o refute cada una de las afirmaciones siguientes:

   (a) Si $\Sigma \models \alpha$ o $\Sigma \models \beta$, entonces $\Sigma \models (\alpha \vee \beta)$.

   (b) Si $\Sigma \models (\alpha \vee \beta)$, entonces $\Sigma \models \alpha$ o $\Sigma \models \beta$.

6. (a) Pruebe que si v_1 y v_2 son asignaciones de verdad que coinciden en todos los símbolos de enunciado de la fórmula α, entonces $\bar{v}_1(\alpha) = \bar{v}_2(\alpha)$. Use el principio de inducción.

   (b) Sea S un conjunto de símbolos de enunciado que contiene todos los que aparecen en Σ y en τ (y posiblemente otros más). Pruebe que $\Sigma \models \tau$ sii toda asignación de verdad para S que satisface todos los elementos de Σ también satisface τ. (Ésta es una consecuencia fácil de la parte (a). Lo interesante de la parte (b) está en que no necesitamos preocuparnos por obtener *exactamente* el dominio de una asignación de verdad si éste es suficientemente grande. Por ejemplo, una opción sería usar siempre asignaciones de verdad para *todos* los símbolos de enunciado. El inconveniente es que éstos son una cantidad infinita de objetos, hay muchos —una cantidad incontable— de ellos.)

7. Está usted en una tierra habitada por gente que o siempre dice la verdad o siempre dice mentiras. Llega usted a una encrucijada en el camino y necesita saber cuál de los dos caminos lleva a la capital. Se encuentra a un residente local que sólo tiene tiempo de responder con un sí o un no a una sola pregunta. ¿Qué pregunta debe usted hacerle para saber cuál de los dos caminos tomar? *Sugerencia:* Haga una tabla.

8. (Sustitución) Consideremos una sucesión $\alpha_1, \alpha_2, \ldots$ de fórmulas. Para una fórmula φ, sea φ^* el resultado de reemplazar el símbolo $\mathbf{A}_n$ por α_n, para cada n.

   (a) Sea v una asignación de verdad para el conjunto de todos los símbolos de enunciado; definimos u como la asignación de verdad para la cual $u(\mathbf{A}_n) = \bar{v}(\alpha_n)$. Pruebe que $\bar{u}(\varphi) = \bar{v}(\varphi^*)$. Use el principio de inducción.

   (b) Pruebe que si φ es una tautología, entonces φ^* también lo es. (Por ejemplo, una de nuestras tautologías selectas es $((\mathbf{A} \wedge \mathbf{B}) \leftrightarrow (\mathbf{B} \wedge \mathbf{A}))$. De aquí podemos concluir, por sustitución, que $((\alpha \wedge \beta) \leftrightarrow (\beta \wedge \alpha))$ es una tautología, para cualesquiera fórmulas α y β.)

9. (Dualidad.) Sea α una fórmula cuyos únicos símbolos de conectivo son $\wedge$, $\vee$ y $\neg$. Sea α^* el resultado de intercambiar $\wedge$ y $\vee$ y reemplazar cada símbolo de enunciado por su negación. Pruebe que α^* es tautológicamente equivalente a $(\neg\, \alpha)$. Use el principio de inducción.

   Observación: Se sigue que si $\alpha \models\!\!\!\dashv \beta$, entonces:
   $$\alpha^* \models\!\!\!\dashv \beta^*.$$

10. Digamos que un conjunto Σ_1 de fórmulas es *equivalente* a un conjunto Σ_2 de fórmulas sii para toda fórmula α, $\Sigma_1 \models \alpha$ sii $\Sigma_2 \models \alpha$. Un conjunto Σ es *independiente* sii ningún elemento de Σ es implicado tautológicamente por el resto de los elementos de Σ. Pruebe que lo siguiente se cumple:
    (a) Todo conjunto finito de fórmulas tiene un subconjunto equivalente independiente.
    (b) Hay conjuntos infinitos que no tienen subconjuntos equivalentes independientes.
    *(c) Sea $\Sigma = \{\sigma_0, \sigma_1, \ldots\}$; pruebe que existe un conjunto equivalente independiente Σ'. (Por la parte (b), no podemos esperar tener $\Sigma' \subseteq \Sigma$ en general.)

11. Muestre que una asignación de verdad v satisface la fórmula:
    $$(\cdots(A_1 \leftrightarrow A_2) \leftrightarrow \cdots \leftrightarrow A_n)$$
    sii $v(A_i) = F$ para un número par de i's, $1 \leq i \leq n$. (Por la ley asociativa para $\leftrightarrow$, la colocación de los paréntesis no es crucial.)

12. Hay tres sospechosos de un asesinato: Arroyo, Bulnes y Carreño. Arroyo declara: "Yo no lo hice. La víctima era un viejo conocido de Bulnes, pero Carreño lo odiaba." Bulnes dice: "Yo no lo hice. Ni siquiera conocía al tipo. Además, no estuve en la ciudad durante esa semana." Carreño dice: "Yo no lo hice. Vi a Arroyo y a Bulnes en la ciudad con la víctima el día del asesinato; uno de ellos tiene que haberlo cometido." Suponga que los dos inocentes están diciendo la verdad, pero que el culpable esté mintiendo. ¿Quién es el asesino?

13. En un anuncio de una revista de tenis se afirma: "Si no estoy jugando tenis, estoy viendo jugar tenis. Y si no estoy viendo jugar tenis, estoy leyendo acerca del tenis." Podemos suponer que el que habla no puede hacer más que una de estas tres actividades en un momento dado. ¿Qué está haciendo? (Traduzca los enunciados dados a nuestro lenguaje formal; considere las posibles asignaciones de verdad.)

14. Sea $\mathcal{S}$ el conjunto de todos los símbolos de enunciado, y suponga que $v : \mathcal{S} \to \{F, V\}$ es una asignación de verdad. Muestre que hay *cuando mucho* una extensión $\overline{v}$ que cumple las condiciones 0-5 listadas al principio de esta sección. (Suponga que $\overline{v}_1$ y $\overline{v}_2$ son tales extensiones. Use el principio de inducción para mostrar que $\overline{v}_1 = \overline{v}_2$.)

15. De las siguientes tres fórmulas, ¿cuál implica tautológicamente a cuál?

(a) $(\mathbf{A} \leftrightarrow \mathbf{B})$

(b) $(\neg((\mathbf{A} \to \mathbf{B}) \to (\neg(\mathbf{B} \to \mathbf{A}))))$

(c) $(((\neg \mathbf{A}) \vee \mathbf{B}) \wedge (\mathbf{A} \vee (\neg \mathbf{B})))$

3. *Un algoritmo de análisis*

El propósito de esta sección es demostrar que hemos usado suficientes paréntesis para eliminar cualquier ambigüedad al analizar las fórmulas. (La existencia de la extensión $\overline{v}$ de una asignación de verdad v dependerá de esta falta de ambigüedad.)[1]

Es instructivo considerar el resultado de no tener ningún paréntesis. La ambigüedad resultante se ilustra con la fórmula

$$\mathbf{A}_1 \vee \mathbf{A}_2 \wedge \mathbf{A}_3,$$

la cual se puede formar de dos maneras, que corresponden a $((\mathbf{A}_1 \vee \mathbf{A}_2) \wedge \mathbf{A}_3)$ y a $(\mathbf{A}_1 \vee (\mathbf{A}_2 \wedge \mathbf{A}_3))$. Si $v(\mathbf{A}_1) = V$ y $v(\mathbf{A}_3) = F$,

[1] El lector que ya ha aceptado la existencia de $\overline{v}$ puede prescindir de casi toda esta sección. La subsección final, sobre omisión de paréntesis, aún será necesaria.

entonces hay un conflicto irresoluble que surge al tratar de calcular $\overline{v}(A_1 \vee A_2 \wedge A_3)$.

Debemos probar que, con nuestros paréntesis, no surge este tipo de ambigüedad; por el contrario, cada fórmula se forma de manera única. Hay un sentido en el que este hecho carece de importancia: si fallara, simplemente cambiaríamos de notación hasta que fuera verdadera. Por ejemplo, en lugar de construir las fórmulas por medio de concatenaciones, podríamos haber usado parejas y ternas ordenadas: $\langle \neg, \alpha \rangle$, $\langle \alpha, \wedge, \beta \rangle$, etc. (Éste es, de hecho, un método limpio, aunque poco tradicional.) Se seguiría, entonces, de inmediato que las fórmulas tienen descomposición única; pero no necesitamos recurrir a este procedimiento y a continuación probaremos que no lo necesitamos.

Lema 13A Toda fórmula tiene el mismo número de paréntesis izquierdos que derechos.

Demostración Esto se hizo como un ejemplo de la sección 1 de este capítulo. ⊣

Lema 13B Cualquier segmento inicial propio de una fórmula tiene un exceso de paréntesis izquierdos. Así, ningún segmento inicial propio de una fórmula puede ser una fórmula.

Demostración Aplicamos el principio de inducción al conjunto S de fórmulas con la propiedad deseada (que sus segmentos iniciales propios tengan más paréntesis izquierdos). Una fórmula que consista en un solo símbolo de enunciado no tiene segmentos iniciales propios y por tanto pertenece a S por vacuidad. Para verificar que S es cerrado bajo $\mathcal{E}_\wedge$, consideremos dos elementos α y β de S. Los segmentos iniciales propios de $(\alpha \wedge \beta)$ son los siguientes:

1. $($.

2. $(\alpha_0$, donde α_0 es un segmento inicial propio de α.

3. $(\alpha$.

4. $(\alpha\wedge$.

5. $(\alpha \wedge \beta_0$, donde β_0 es un segmento inicial propio de β.

6. $(\alpha \wedge \beta$.

Aplicando la hipótesis inductiva de que α y β están en S (en los casos 2 y 5), obtenemos la conclusión deseada. Para la cerradura bajo las otras cuatro operaciones de construcción de fórmulas, el argumento es similar. ⊣

Un algoritmo de análisis

Ahora vamos a describir un procedimiento que, dada una expresión, determinará si la expresión es una fórmula permitida y, si lo es, construirá el árbol que muestra cómo fue formada a partir de símbolos de enunciado y aplicando las operaciones de construcción de fórmulas. Además veremos que este árbol está *unívocamente determinado* por la fórmula. Este último hecho es lo que nos asegurará que tenemos suficientes paréntesis para una notación no ambigua.

Supongamos entonces que se nos da una expresión. Construimos un árbol con esa expresión en el vértice. Inicialmente es el único vértice del árbol; pero según progresa el procedimiento, el árbol crecerá hacia abajo a partir de la expresión dada. Como ejemplo, imaginemos el árbol de la sección 1 de este capítulo (p. 35).

El algoritmo consiste en los siguientes cuatro pasos:

1. Si todos los vértices minimales (los de la parte de abajo) tienen símbolos de enunciado, entonces el procedimiento ha terminado. (La expresión dada es ciertamente una fórmula, y hemos construido su árbol.) Si no es así, elija un vértice minimal con una expresión que no sea un símbolo de enunciado. Examinamos esa expresión.

2. El primer símbolo debe* ser (. Si el segundo símbolo es el símbolo de negación, vaya directamente al paso 4. De otra forma, siga al paso 3.

3. Recorra la expresión desde la izquierda hasta llegar a $(\alpha$, donde α es una expresión con igual número de paréntesis iz-

* Si esto no ocurre, entonces la expresión original no es una fórmula. Rechazamos la expresión dada arguyendo que no es una fórmula y terminamos.

quierdos que derechos.† Entonces α es el primero de los dos componentes. El siguiente símbolo debe* ser $\wedge$, $\vee$, $\rightarrow$ o $\leftrightarrow$. Éste es el conectivo principal. El resto de la expresión, $\beta)$, debe* consistir en una expresión β y un paréntesis derecho. Extendemos el árbol creando dos nuevos vértices bajo el vértice actual, con α como la expresión del vértice "hijo izquierdo", y β como la expresión del vértice "hijo derecho". Regrese al paso 1.

4. Ahora se sabe que los primeros dos símbolos son $(\neg$. El resto de la expresión, $\beta)$, debe* consistir en una expresión β y un paréntesis derecho. Extendemos el árbol creando un nuevo vértice debajo del actual, con β como la expresión en el vértice hijo. Regrese al paso 1.

A continuación se plantean algunos comentarios para apoyar la correctud de este algoritmo.

En primer lugar, dada cualquier expresión, el procedimiento termina después de un número finito de pasos. Esto obedece a que cualquier vértice contiene una expresión más corta que la de arriba de él, y así la profundidad del árbol está acotada por la longitud de la expresión dada.

En segundo lugar, las elecciones hechas por el procedimiento no podrían haber sido de otra manera. Por ejemplo, en el paso 3 llegamos a una expresión α. No podríamos usar menos de α como componente, ya que no habría balance entre paréntesis derechos e izquierdos (como lo exige el lema 13A). No podríamos usar nada además de α, porque esto contendría el segmento inicial propio α que estaba balanceado (lo cual violaría el lema 13B). Por tanto, sólo podemos usar α, y entonces la elección del conectivo principal es inevitable. Concluimos que este algoritmo construye el *único* árbol posible para la expresión dada.

En tercer lugar, si el algoritmo usa las notas a pie de página para rechazar la expresión dada, entonces la expresión no podría haber sido una fórmula: el rechazo es correcto. Esto se debe a que fracasó el único intento posible para construir su árbol.

† Si se llega al final de la expresión antes de encontrar tal α, entonces la expresión original no era una fórmula. Rechazamos la expresión dada por no ser una fórmula y terminamos.

* Si esto no ocurre, entonces la expresión original no es una fórmula. Rechazamos la expresión dada arguyendo que no es una fórmula y terminamos.

Finalmente, si el algoritmo no usa las notas a pie de página para rechazarla, entonces la expresión dada es de verdad una fórmula permitida. Eso obedece a que *tenemos* su árbol; recorriendo el árbol de abajo hacia arriba, descubrimos inductivamente que todo vértice tiene una fórmula, incluido el vértice superior.

La segunda de las observaciones anteriores nos permite concluir que nuestro lenguaje tiene suficientes paréntesis; cada fórmula tiene un *único* árbol de la clase aquí construida. Tenemos "unicidad de la lectura", y no sólo *existe* un único árbol para cada fórmula, sino que sabemos cómo construirlo; podemos llevar a cabo este algoritmo usando suficiente papel.

Ahora bien, regresando al problema de la existencia de la extensión $\bar{v}$ de una asignación de verdad v: la unicidad de los árboles es aquí el hecho crucial. Para cualquier fórmula φ hay un único árbol que la construye. Al recorrer este árbol de abajo hacia arriba, asignando un valor de verdad $\bar{v}(\alpha)$ a cada vértice α, podemos llegar sin ambigüedad a un valor para $\bar{v}(\varphi)$. Además, la función descrita de *este* modo cumple las condiciones 0–5 listadas al principio de la sección 2 de este capítulo. Y no sólo eso, sino que, dados φ y los valores de v en sus símbolos de enunciado, sabemos cómo llevar a cabo el cálculo de $\bar{v}(\varphi)$.

Así, usando el algoritmo de análisis, podemos construir una función $\bar{v}$ como se describió en el teorema 12A. Y sólo puede haber una tal $\bar{v}$; confróntese el ejercicio 14 de la sección 2.

La única razón por la que la existencia de $\bar{v}$ es de algún modo un problema es que en la sección 2 de este capítulo se describe por *recursión*; es decir, $\bar{v}(\varphi)$ se especifica haciendo uso de la misma función $\bar{v}$, aplicada a fórmulas menores. En la próxima sección abordaremos el asunto de definir una función por recursión de manera más general. Al tratar el tema en forma más abstracta podremos aislar mejor lo que está en juego.

Notación polaca

Es posible evitar a la vez la ambigüedad y los paréntesis; esto se puede lograr mediante un recurso muy sencillo. Por ejemplo, en lugar de $(\alpha \wedge \beta)$, usamos $\wedge\alpha\beta$. Sea el conjunto de P-fórmulas el conjunto generado a partir de los símbolos de enunciado

mediante las cinco operaciones

$$\mathcal{D}_{\neg}(\alpha) = \neg\,\alpha, \qquad \mathcal{D}_{\vee}(\alpha,\beta) = \vee\alpha\beta,$$
$$\mathcal{D}_{\wedge}(\alpha,\beta) = \wedge\alpha\beta, \quad \mathcal{D}_{\rightarrow}(\alpha,\beta) = \rightarrow\alpha\beta,$$
$$\mathcal{D}_{\leftrightarrow}(\alpha,\beta) = \leftrightarrow\alpha\beta.$$

Por ejemplo,

$$\rightarrow \wedge\, \mathbf{AD} \vee \neg\, \mathbf{B} \leftrightarrow \mathbf{CB}$$

es una P-fórmula.

Aquí es bastante notoria la necesidad de un algoritmo para analizar la estructura. Aun para el breve ejemplo anterior se requiere alguna reflexión para ver cómo se construyó. En la sección 3 del capítulo II daremos un teorema de unicidad de lectura de tales expresiones.

Esta manera de escribir fórmulas (pero con N, K, A, C y E en lugar de $\neg$, $\wedge$, $\vee$, $\rightarrow$ y $\leftrightarrow$, respectivamente) fue introducida por el lógico polaco Jan Lukasiewicz. La notación es adecuada para el procesamiento automático. Los programas compiladores de computadoras comienzan a menudo por la conversión de las fórmulas a notación polaca.

Omisión de paréntesis

De aquí en adelante, cuando nombremos fórmulas, no nos sentiremos obligados a mencionar explícitamente todos los paréntesis. Para establecer una notación más compacta adoptaremos ahora las siguientes convenciones:

1. El primero y el último de los paréntesis no necesitan ser mencionados. Por ejemplo, cuando escribimos "$\mathbf{A} \wedge \mathbf{B}$" nos referimos a $(\mathbf{A} \wedge \mathbf{B})$.

2. El símbolo de negación se aplica a lo menos que sea posible. Por ejemplo, $\neg\,\mathbf{A} \wedge \mathbf{B}$ es $(\neg\mathbf{A}) \wedge \mathbf{B}$, o sea $((\neg\mathbf{A}) \wedge \mathbf{B})$. Esto no es lo mismo que $(\neg(\mathbf{A} \wedge \mathbf{B}))$.

3. La conjunción y la disyunción se aplican a lo menos que sea posible, siempre y cuando se observe la convención 2. Por ejemplo,

$$\mathbf{A} \wedge \mathbf{B} \rightarrow \neg\,\mathbf{C} \vee \mathbf{D} \quad \text{es} \quad ((\mathbf{A} \wedge \mathbf{B}) \rightarrow ((\neg\,\mathbf{C}) \vee \mathbf{D})).$$

4. Cuando se usa repetidamente un símbolo de conectivo, la agrupación se efectúa a la derecha:

$$\alpha \wedge \beta \wedge \gamma \quad \text{es} \quad \alpha \wedge (\beta \wedge \gamma),$$
$$\alpha \rightarrow \beta \rightarrow \gamma \quad \text{es} \quad \alpha \rightarrow (\beta \rightarrow \gamma).$$

Se debe admitir que estas convenciones quebrantan lo que se dijo antes acerca de los nombres de las expresiones. Podemos darnos esta licencia sólo porque ya no nos interesa nombrar expresiones que no sean fórmulas.

Ejercicios

1. Reescriba las tautologías de la lista "Algunas tautologías selectas" que aparece al final de la sección 2 de este capítulo, pero usando las convenciones de esta sección para minimizar el número de paréntesis.

2. Dé un ejemplo de fórmulas α y β y expresiones γ y δ tales que $(\alpha \wedge \beta) = (\gamma \wedge \delta)$, pero $\alpha \neq \gamma$.

3. Desarrolle el argumento para el lema 13B en el caso de la operación $\mathcal{E}_{\neg}$.

4. Suponga que modificamos nuestra definición de fórmula omitiendo todos los paréntesis *derechos*. Así, en lugar de

$$((\mathbf{A} \wedge (\neg \mathbf{B})) \rightarrow (\mathbf{C} \vee \mathbf{D}))$$

usamos

$$((\mathbf{A} \wedge (\neg \mathbf{B} \rightarrow (\mathbf{C} \vee \mathbf{D}.$$

Pruebe que aún tenemos unicidad de la lectura (es decir, cada fórmula sigue teniendo sólo una descomposición posible). *Sugerencia:* Estas expresiones tienen el mismo número de paréntesis que de símbolos de conectivo.

5. En la lengua española se usan conectivos que constan de dos partes: "tanto... como...", "o bien..., o bien...", "si..., entonces..." ¿Cómo afecta esto a la unicidad de la lectura en español?

6. Hemos proporcionado un algoritmo para analizar una fórmula por medio de la construcción de su árbol de arriba hacia abajo. También hay formas de construir el árbol de abajo hacia arriba; esto se puede lograr buscando en la fórmula las parejas más interiores de paréntesis. Dé una descripción completa de un algoritmo de este tipo.

7. Suponga que los paréntesis izquierdo y derecho son indistinguibles uno de otro. Así, en vez de $(\alpha \vee (\beta \wedge \gamma))$, tenemos $|\alpha \vee |\beta \wedge \gamma||$. ¿Aún tienen las fórmulas una descomposición única?

4. *Inducción y recursión*[2]

Inducción

Hay un tipo especial de construcción que aparece frecuentemente en lógica y en otras ramas de las matemáticas. Puede ocurrir que queramos construir cierto subconjunto de un conjunto U comenzando por algunos elementos iniciales de U y aplicando ciertas operaciones una y otra vez. El conjunto que buscamos será el conjunto más pequeño que contenga los elementos iniciales y que sea cerrado bajo las operaciones. Sus elementos serán aquellos elementos de U que se pueden construir a partir de los elementos iniciales aplicando las operaciones un número finito de veces.

En el caso especial de interés inmediato para nosotros, U es el conjunto de las expresiones, los elementos iniciales son los símbolos de enunciado y las operaciones son $\mathcal{E}_{\neg}$, $\mathcal{E}_{\wedge}$, etc. El conjunto que se va a construir es el de las fórmulas; pero más adelante encontraremos otros casos especiales y será de utilidad estudiar aquí la situación en abstracto.

Para simplificar la discusión, consideraremos un conjunto inicial $B \subseteq U$ y una clase $\mathcal{F}$ de funciones con sólo dos elementos f y g, donde

$$f: U \times U \to U \quad \text{y} \quad g: U \to U.$$

[2] Por un lado, los conceptos de esta sección son importantes y surgen en todas las áreas de las matemáticas. Por otro lado, tal vez los lectores quieran posponer —no saltar— el estudio de esta sección.

Así, f es una operación binaria sobre U y g es una operación unaria. (De hecho, $\mathcal{F}$ no necesariamente debe ser finita; se verá que la presente discusión simplificada es aplicable a una situación más general. $\mathcal{F}$ puede ser cualquier conjunto de relaciones en U, y en el capítulo II usaremos este mayor nivel de generalidad. No obstante, el caso discutido aquí es más fácil de visualizar y es lo suficientemente general para ilustrar las ideas. Para una versión menos limitada, véase el ejercicio 3.)

Si a y b pertenecen a B, entonces el conjunto C que queremos construir tendrá, por ejemplo, los elementos

$$b, \quad f(b,b), \quad g(a), \quad f(g(a),f(b,b)), \quad g(f(g(a),f(b,b))).$$

Por supuesto que estos elementos pueden no ser distintos. La idea es que se nos han dado ciertos ladrillos y ciertos tipos de mortero, y queremos que C contenga solamente las cosas que somos capaces de construir.

Al definir C más formalmente, tenemos la posibilidad de escoger entre dos definiciones. Podemos definirlo "de arriba abajo" como sigue: Llamemos a un subconjunto S de U *cerrado* bajo f y g sii siempre que los elementos x y y pertenecen a S, entonces también $f(x,y)$ y $g(x)$ pertenecen a S. Llamemos *inductivo* a S sii $B \subseteq S$ y S es cerrado bajo f y g. Sea C^* la intersección de todos los subconjuntos inductivos de U; así, $x \in C^*$ sii x pertenece a todo subconjunto inductivo de U. No es difícil advertir (y el lector debería verificarlo) que C^* es inductivo. Aún más, C^* es el conjunto inductivo más pequeño que está contenido en todos los demás conjuntos inductivos.

La segunda definición (que es equivalente) va "de abajo arriba". Queremos que los elementos de C_* sean todas las cosas que se pueden alcanzar desde B aplicando f y g un número finito de veces. Por el momento definimos una *sucesión de construcción* como una sucesión finita $\langle x_1, \ldots, x_n \rangle$ de elementos de U tales que para cada $i \leq n$ se cumple por lo menos una de las siguientes condiciones:

$x_i \in B$,

existen $j < i$, $k < i$, tales que $x_i = f(x_j, x_k)$,

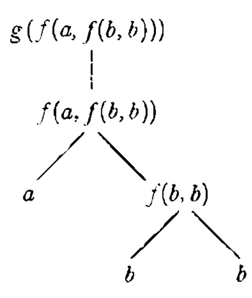
existe $j < i$, tal que $x_i = g(x_j)$.

En otras palabras, cada elemento de la sucesión o está en B o es el resultado de aplicar f o g a elementos *anteriores*. Entonces, sea C_* el conjunto de todos los puntos x tales que alguna sucesión de construcción termina con x.

Sea C_n el conjunto de todos los puntos x tales que alguna sucesión de construcción de longitud n termina con x. Entonces $C_1 = B$,

$$C_1 \subseteq C_2 \subseteq C_3 \subseteq \cdots,$$

y $C_* = \bigcup_n C_n$. Por ejemplo, $g(f(a, f(b, b)))$ pertenece a C_5 y por tanto pertenece a C_*, como se puede apreciar en el siguiente árbol:



Al aplanar este árbol hasta convertirlo en un orden lineal se obtiene una sucesión de construcción $g(f(a, f(b, b)))$.

EJEMPLOS

1. Los números naturales. Sea U el conjunto de todos los números reales y sea $B = \{0\}$. Tomemos una operación S, donde $S(x) = x + 1$. Entonces

   $$C_* = \{0, 1, 2, \ldots\}.$$

   El conjunto C_* de los números naturales tiene como elementos exactamente aquellos números que se pueden obtener a partir del 0 aplicando repetidamente la operación sucesor.

2. Los enteros. Sea U el conjunto de todos los números reales; sea $B = \{0\}$. Esta vez tomemos dos operacio-

nes, la operación sucesor S y la operación predecesor P:

$$S(x) = x + 1 \quad \text{y} \quad P(x) = x - 1.$$

Ahora C_* es el conjunto de todos los enteros,

$$C_* = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Nótese que hay más de una manera de obtener el 2 como elemento de C_*, ya que el 2 es $S(S(0))$, pero también es $S(P(S(S(0))))$.

3. Las funciones algebraicas. Sea U el conjunto de todas las funciones cuyo dominio y rango son ambos conjuntos de números reales. Sea B el conjunto cuyos elementos son la función identidad y todas las funciones constantes. Sea $\mathcal{F}$ el conjunto cuyos elementos son las operaciones (sobre funciones) de suma, multiplicación, división y extracción de raíz. Entonces C_* es una clase de funciones algebraicas.

4. Las fórmulas. Sea U el conjunto de todas las expresiones y sea B el conjunto de los símbolos de enunciado. Sea $\mathcal{F}$ el conjunto de las cinco operaciones de construcción de fórmulas: $\mathcal{E}_\neg$, $\mathcal{E}_\wedge$, $\mathcal{E}_\vee$, $\mathcal{E}_\rightarrow$ y $\mathcal{E}_\leftrightarrow$. Entonces C_* es el conjunto de todas las fórmulas.

En este momento deberíamos verificar que nuestras dos definiciones son de hecho equivalentes, es decir que $C^* = C_*$.

Para probar que $C^* \subseteq C_*$ sólo necesitamos verificar que C_* es inductivo; es decir, que $B \subseteq C_*$ y que C_* es cerrado bajo las funciones. Es evidente que $B = C_1 \subseteq C_*$. Si x y y están en C_*, entonces podemos concatenar sus sucesiones de construcción y agregar al final $f(x, y)$ para obtener una sucesión de construcción que coloca a $f(x, y)$ en C_*. De igual manera, C_* es cerrado bajo g.

Finalmente, para probar que $C_* \subseteq C^*$ consideramos un elemento de C_* y una sucesión de construcción $\langle x_0, \ldots, x_n \rangle$ para él. Por inducción común y corriente sobre i, podemos ver que $x_i \in C^*$, si $i \leq n$. En primer lugar, $x_0 \in B \subseteq C^*$. Para el paso

inductivo se usa el hecho de que C^* es cerrado bajo las funciones. De esta manera concluimos que

$$\bigcup_n C_n = C_* = C^* = \bigcap\{S \mid S \text{ es inductivo}\}.$$

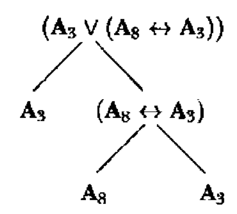
(Una observación parentética: supongamos que el presente estudio estuviera inserto en la teoría axiomática de conjuntos, en la que los números naturales generalmente se definen de arriba abajo. Entonces nuestra definición de C_* (que usa la finitud y por tanto los números naturales) no difiere realmente de nuestra definición de C^*. Sin embargo, no estamos trabajando dentro de la teoría axiomática de conjuntos, sino dentro de la matemática intuitiva. Y la noción de número natural parece ser un concepto intuitivo sólido y bien entendido.)

Como $C^* = C_*$, llamamos a este conjunto C simplemente y nos referimos a él como el conjunto *generado a partir de* B *por* las funciones que pertenecen a $\mathcal{F}$. En la demostración de muchos teoremas usaremos el siguiente:

Principio de inducción Sea C el conjunto generado a partir de B por las funciones que pertenecen a $\mathcal{F}$. Si S es un subconjunto de C que contiene a B y es cerrado bajo las funciones que pertenecen a $\mathcal{F}$, entonces $S = C$.

Demostración S es inductivo, por lo que $C = C^* \subseteq S$. La otra inclusión está entre las hipótesis. ⊣

El caso especial que ahora nos interesa es, por supuesto, el ejemplo 4. Aquí C es la clase de las fórmulas generadas a partir del conjunto de los símbolos de enunciado por las operaciones de construcción de fórmulas. Este caso especial tiene propiedades interesantes. Tanto α como β son segmentos propios de $\mathcal{E}_\wedge(\alpha, \beta)$; es decir, de $(\alpha \wedge \beta)$. En general, si observamos el árbol genealógico de una fórmula, veremos que cada componente es un segmento propio del producto final.



Supongamos, por ejemplo, que por el momento llamamos *especial* a una expresión si los únicos símbolos de enunciado que aparecen en ella están entre $\{A_2, A_3, A_5\}$ y los únicos conectivos que figuran en ella están entre $\{\neg, \rightarrow\}$. Entonces, ninguna fórmula especial requiere ni A_9 ni $\mathcal{E}_\wedge$ para su construcción. De hecho, toda fórmula especial pertenece al conjunto C_s generado a partir de $\{A_2, A_3, A_5\}$ por $\mathcal{E}_\neg$ y $\mathcal{E}_\rightarrow$. (Podemos usar el principio de inducción para probar que toda fórmula o bien pertenece a C_s, o bien no es especial.)

Recursión

Regresemos al caso más abstracto. Tenemos un conjunto U (como el conjunto de todas las expresiones), un subconjunto B de U (como el conjunto de los símbolos de enunciado) y dos funciones f y g, donde

$$f : U \times U \rightarrow U \quad \text{y} \quad g : U \rightarrow U.$$

C es el conjunto generado a partir de B por f y g.

El problema que ahora queremos considerar es el de definir recursivamente una función sobre C. Esto es, suponemos que nos han sido dadas:

1. Reglas para calcular $\overline{h}(x)$ para $x \in B$.

2a. Reglas para calcular $\overline{h}(f(x, y))$ usando $\overline{h}(x)$ y $\overline{h}(y)$.

2b. Reglas para calcular $\overline{h}(g(x))$ usando $\overline{h}(x)$.

(Por ejemplo, ésta es la situación discutida en la sección 2 de este capítulo, donde $\overline{h}$ es la extensión de una asignación de verdad para B.) No es difícil ver que a lo sumo puede haber

una función $\bar{h}(x)$ sobre C que satisfaga todas las condiciones dadas.

Pero es posible que no exista tal función; las reglas pueden ser contradictorias. Por ejemplo, sean

$$\begin{aligned} U &= \text{el conjunto de los números reales}, \\ B &= \{0\}, \\ f(x, y) &= x \cdot y, \\ g(x) &= x + 1. \end{aligned}$$

Entonces C es el conjunto de los números naturales. Supongamos que imponemos las siguientes condiciones a $\bar{h}$:

1. $\bar{h}(0) = 0$.
2a. $\bar{h}(f(x, y)) = f(\bar{h}(x), \bar{h}(y))$.
2b. $\bar{h}(g(x)) = \bar{h}(x) + 2$.

Entonces no puede existir tal función $\bar{h}$. (Intente calcular $\bar{h}(1)$ y observe que tenemos a la vez $1 = g(0)$ y $1 = f(g(0), g(0))$.)

En álgebra encontramos una situación similar.[3] Supóngase que tenemos un grupo G generado a partir de B por la multiplicación del grupo y la extracción de inverso. Entonces una función arbitraria de B en un grupo H no necesariamente se puede extender a un homomorfismo de todo el grupo G en H. Pero en caso de que G sea un grupo libre con B como conjunto de generadores independientes, entonces cualquier función de ese tipo se puede extender a un homomorfismo de todo el grupo.

Se dice que C está generado *libremente* a partir de B por f y g sii, además de satisfacer los requisitos para que esté generado, f_C y g_C, las restricciones de f y de g a C, cumplen las siguientes condiciones:

1. f_C y g_C son uno a uno.

[3] Esperamos que ejemplos como éste sean de utilidad para el lector que ya tenga alguna experiencia algebraica. Los demás se alegrarán de saber que estos ejemplos son solamente ilustrativos y no son esenciales a nuestra exposición.

2. El rango de f_G el rango de g_C y el conjunto B son disjuntos dos a dos.

El resultado principal de esta sección, el teorema de recursión, dice que si C está generado libremente, entonces la función h sobre B siempre tiene una extensión $\bar{h}$ sobre C que sigue la clase de reglas antes consideradas.

Teorema de recursión Supongamos que el subconjunto C de U está libremente generado a partir de B por f y g, donde

$$f: U \times U \to U,$$
$$g: U \to U.$$

Supongamos, además, que V es un conjunto y F, G y h son funciones tales que

$$h : B \to V,$$
$$F : V \times V \to V,$$
$$G : V \to V.$$

Existe entonces una única función

$$\bar{h} : C \to V$$

tal que

(i) Para toda $x \in B$, $\bar{h}(x) = h(x)$.

(ii) Para $x, y \in C$,

$$\bar{h}(f(x, y)) = F(\bar{h}(x), \bar{h}(y)),$$
$$\bar{h}(g(x)) = G(\bar{h}(x)).$$

Vista algebraicamente, la conclusión del teorema dice que cualquier función h de B en V se puede extender a un homomorfismo $\bar{h}$ de C (con las operaciones f y g) en V (con las operaciones F y G).

Si el contenido del teorema de recursión no queda claro de inmediato, intentemos verlo cromáticamente. Queremos tener una función $\bar{h}$ que pinte a cada elemento de C de algún color. Tenemos ante nosotros:

1. h, que nos indica cómo colorear los elementos iniciales de B;

2. F, que nos dice cómo combinar el color de x y de y para obtener el color de $f(x, y)$ (es decir, esto da $\bar{h}(f(x, y))$ en términos de $\bar{h}(x)$ y $\bar{h}(y)$);

3. G, que igualmente nos dice cómo convertir el color de x en color de $g(x)$.

El peligro es que haya un conflicto en que, por ejemplo, F diga "verde" pero G diga "rojo" para el mismo punto (que tenga la mala fortuna de ser igual tanto a $f(x, y)$ como a $g(z)$ para algunas x, y, z). Pero si C está generado *libremente*, se evita el peligro.

Ejemplos Consideremos de nuevo los ejemplos de la subsección anterior.

1. $B = \{0\}$ con una operación, la operación sucesor S. Entonces C es el conjunto $\mathbb{N}$ de los números naturales. Puesto que la operación sucesor es uno a uno y 0 no está en su rango, C está generado libremente a partir de $\{0\}$ por S. Así, por el teorema de recursión, dado cualquier conjunto V, cualquier $a \in V$, y cualquier $F : V \to V$, existe una única $\bar{h} : \mathbb{N} \to V$ tal que $\bar{h}(0) = a$ y $\bar{h}(S(x)) = F(\bar{h}(x))$ para cada $x \in \mathbb{N}$. Por ejemplo, existe una única $\bar{h} : \mathbb{N} \to \mathbb{N}$ tal que $\bar{h}(0) = 0$ y $\bar{h}(S(x)) = 1 - \bar{h}(x)$. Esta función adopta el valor 0 en los números pares y el valor 1 en los números impares.

2. Los enteros están generados a partir de $\{0\}$ por las operaciones de sucesor y predecesor, pero no libremente.

3. La condición de libertad tampoco se cumple para la generación de las funciones algebraicas tal como se describió anteriormente.

4. Las fórmulas están generadas libremente a partir de los símbolos de enunciado por las cinco operaciones de construcción de fórmulas. Este hecho está implícito en el algoritmo de análisis de la sección anterior; ahora queremos concentrarnos en él aquí:

Teorema de la unicidad de la lectura Las cinco operaciones de construcción de fórmulas, cuando se restringen al conjunto de las fórmulas,

(a) tienen rangos disjuntos entre sí y disjuntos del conjunto de los símbolos de enunciado, y

(b) son uno a uno.

En otras palabras, el conjunto de las fórmulas está *libremente* generado a partir del conjunto de símbolos de enunciado por las cinco operaciones.

Demostración Para mostrar que la restricción de $\mathcal{E}_\wedge$ es uno a uno, supongamos que

$$(\alpha \wedge \beta) = (\gamma \wedge \delta),$$

donde α, β, γ y δ son fórmulas. Borremos el primer símbolo de cada sucesión y obtendremos

$$\alpha \wedge \beta) = \gamma \wedge \delta).$$

Entonces debemos tener que $\alpha = \gamma$, para que ninguno de ellos sea un segmento inicial propio del otro (en contradicción con el lema 13B). Y luego se sigue en forma inmediata que $\beta = \delta$. El mismo argumento se aplica a $\mathcal{E}_\vee$, $\mathcal{E}_\rightarrow$ y $\mathcal{E}_\leftrightarrow$; para $\mathcal{E}_\neg$ basta un argumento más simple.

Un razonamiento similar nos dice que las operaciones tienen rangos ajenos (o disjuntos). Por ejemplo, si

$$(\alpha \wedge \beta) = (\gamma \rightarrow \delta)$$

donde α, β, γ y δ son fórmulas, entonces, como en el párrafo anterior, tenemos que $\alpha = \gamma$. Pero esto implica que $\wedge = \rightarrow$, lo cual contradice el hecho de que nuestros símbolos son distintos. Por lo tanto, $\mathcal{E}_\wedge$ y $\mathcal{E}_\rightarrow$ (restringidas a fórmulas) tienen rangos ajenos. Y lo mismo vale para cualesquiera dos conectivos binarios.

Los casos restantes son sencillos. Si $(\neg\alpha) = (\beta \wedge \gamma)$, entonces β empieza con $\neg$, lo cual no sucede para ninguna fórmula. Ningún símbolo de enunciado es una sucesión de símbolos que empiece con (. ⊣

Regresemos ahora a la cuestión de extender una asignación de verdad v a $\overline{v}$. Consideremos primero el caso especial donde v es una asignación de verdad para el conjunto de todos los símbolos de enunciado. Por consiguiente, aplicando el teorema de unicidad de la lectura y el teorema de recursión, concluimos que hay una única extensión $\overline{v}$ para el conjunto de todas las fórmulas que tiene las propiedades deseadas.

A continuación tomemos el caso general en que v es una asignación de verdad para un conjunto S de símbolos de enunciado. El conjunto $\overline{S}$ generado a partir de S por las cinco operaciones de construcción de fórmulas está generado libremente, como consecuencia del teorema de unicidad de la lectura. Así, por el teorema de recursión, hay una única extensión $\overline{v}$ de v para dicho conjunto, con las propiedades deseadas.

Ejemplo Podemos aplicar el teorema de recursión para establecer que hay una única función $\overline{h}$ definida en el conjunto de las fórmulas tal que

$$\overline{h}(A) = 1 \text{ si } A \text{ es un símbolo de enunciado,}$$
$$\overline{h}((\neg\alpha)) = 3 + \overline{h}(\alpha),$$
$$\overline{h}((\alpha \wedge \beta)) = 3 + \overline{h}(\alpha) + \overline{h}(\beta),$$

y de igual forma para $\vee$, $\rightarrow$ y $\leftrightarrow$. Esta función da la longitud de cada fórmula.

Demostración del teorema de recursión La idea es construir $\overline{h}$ como la unión de muchas funciones aproximativas. Por el momento llamemos a una función v (que va de un subconjunto de C en V) *aceptable* si satisface las condiciones (i) y (ii) que hemos impuesto a $\overline{h}$. De manera más precisa, v es aceptable sii el dominio de v es un subconjunto de C, su rango un subconjunto de V y para cualesquiera x y y en C:

(i′) Si $x \in B \cap \operatorname{dom} v$, entonces $v(x) = h(x)$.

(ii′) Si $f(x, y) \in \operatorname{dom} v$, entonces x y y también pertenecen a $\operatorname{dom} v$, y $v(f(x, y)) = F(v(x), v(y))$. Si $g(x) \in \operatorname{dom} v$, entonces también $x \in \operatorname{dom} v$, y $v(g(x)) = G(v(x))$.

Sea K la colección de todas las funciones aceptables, y sea $\overline{h} = \bigcup K$ la unión de todas las funciones aceptables. Por tanto,

$$\begin{aligned} \langle x, z\rangle \in \overline{h} \quad &\text{sii} \quad \langle x, z\rangle \text{ pertenece a alguna } v \text{ aceptable} \qquad (*) \\ &\text{sii} \quad v(x) = z \text{ para alguna } v \text{ aceptable.} \end{aligned}$$

Afirmamos que $\overline{h}$ satisface nuestras condiciones. El argumento es conjuntista y comprende cuatro pasos. Para empezar esbozaremos los cuatro pasos:

1. Afirmamos que $\overline{h}$ es una función (es decir, que es de un solo valor). Sea

$$\begin{aligned} S &= \{x \in C \mid \text{para a lo más una } z,\ \langle x,z\rangle \in \overline{h}\,\} \\ &= \{x \in C \mid \text{todas las funciones aceptables} \\ &\qquad \text{definidas en } x \text{ coinciden en } x\} \end{aligned}$$

Es fácil verificar que S es inductivo, usando (i′) y (ii′). Por tanto, $S = C$ y $\overline{h}$ es una función.

2. Afirmamos que $\overline{h} \in K$; es decir, que $\overline{h}$ es una función aceptable. Esto se sigue muy fácilmente de la definición de $\overline{h}$ y del hecho de que sea una función.

3. Afirmamos que $\overline{h}$ está definida en todo C. Basta probar que el dominio de $\overline{h}$ es inductivo. Aquí es donde se usa la hipótesis de libertad. Por ejemplo, un caso es el siguiente: supongamos que x está en el dominio de $\overline{h}$. Entonces $\overline{h}; \langle g(x), G(\overline{h}(x))\rangle$ es aceptable. (Se requiere la libertad para probar que es aceptable.) En consecuencia, $g(x)$ pertenece al dominio de $\overline{h}$. 4. Afirmamos que $\overline{h}$ es única. Dadas dos funciones tales, sea S el conjunto en que coinciden. Entonces S es inductivo y, por tanto, igual a C. ⊣

Veamos ahora los detalles.

1. Como antes, sea

$$\begin{aligned} S &= \{x \in C \mid \text{para a lo más una } z,\ \langle x,z\rangle \in \overline{h}\,\} \\ &= \{x \in C \mid \text{todas las funciones aceptables} \\ &\qquad \text{definidas en } x \text{ coinciden en } x\} \end{aligned}$$

Para mostrar que S es inductivo, primero consideremos algún x en B. Supongamos que v_1 y v_2 son funciones aceptables definidas en x; buscamos mostrar que $v_1(x) = v_2(x)$. Pero la condición (i′) nos dice que ambos $v_1(x)$ y $v_2(x)$ deben ser iguales a $h(x)$, entonces de hecho $v_1(x) = v_2(x)$. Esto muestra que $x \in S$; pero ya que x fue un elemento arbitrario de B, tenemos que $B \subseteq S$.

En segundo lugar, debemos verificar que S está cerrado bajo f y g. Supongamos entonces que algún x y algún y están en S; nos preguntamos si $f(x, y)$ está en S. Supongamos luego que v_1 y v_2 son funciones aceptables definidas en $f(x, y)$; buscamos mostrar que coinciden ahí. Pero la condición (ii′) nos dice que $v_1(f(x,y)) = F(v_1(x),v_1(y))$ y que $v_2(f(x,y)) = F(v_2(x),v_2(y))$. Y como x y y están en S, tenemos que $v_1(x) = v_2(x)$ y que $v_1(y) = v_2(y)$ (y están definidas). Así, concluimos que $v_1(f(x, y)) = v_2(f(x, y))$. Esto muestra que $f(x,y) \in S$. Por lo tanto, S está cerrado bajo f. Un argumento similar muestra que S está cerrado bajo g.

Por lo tanto, S es inductivo y entonces $S = C$. Esto muestra que $\bar{h}$ da un solo valor a cada x, es decir, es una función. Como $\bar{h}$ incluye toda función aceptable como subconjunto, podemos decir que

$$\bar{h}(x) = v(x)$$

siempre que v sea una función aceptable y $x \in \operatorname{dom} v$.

2. Afirmamos que $\bar{h}$ es aceptable. Claramente $\operatorname{dom}\bar{h} \subseteq C$ y $\operatorname{ran}\bar{h} \subseteq V$ (por (∗)) y acabamos de verificar que $\bar{h}$ es una función. Falta verificar que $\bar{h}$ satisface las condiciones (i′) y (ii′).

Primero examinamos (i′). Supongamos que $x \in B$ y $x \in \operatorname{dom}\bar{h}$ (así que $\langle x, \bar{h}(x)\rangle \in \bar{h}$). Debe haber alguna v aceptable tal que $v(x) = \bar{h}(x)$. Como v satisface (i′), tenemos que $v(x) = h(x)$ de donde $\bar{h}(x) = h(x)$. Así, $\bar{h}$ satisface (i′).

Luego examinamos (ii′). Supongamos que $f(x, y) \in \operatorname{dom}\bar{h}$. Otra vez debe haber alguna v aceptable tal que $v(f(x,y)) = \bar{h}(f(x, y))$. Como v satisface (ii′), tenemos

que $v(f(x,y)) = F(v(x),v(y))$. Ahora $\bar{h}(x) = v(x)$ y $\bar{h}(y) = v(y)$ y por lo tanto

$$\bar{h}(f(x,y)) = v(f(x,y)) = F(v(x),v(y)) = F(\bar{h}(x),\bar{h}(y)).$$

De modo similar, encontramos que $\bar{h}(g(x)) = G(\bar{h}(x))$ siempre que $g(x) \in \operatorname{dom}\bar{h}$. Por lo tanto, $\bar{h}$ cumple la condición (ii′) y entonces es aceptable.

3. En seguida debemos mostrar que $\operatorname{dom}\bar{h}$ es inductivo. Primero consideramos un punto x en B. Luego el conjunto $\{\langle x, h(x)\rangle\}$ es una (pequeña) función aceptable, pues claramente satisface (i′). También satisface (ii′) porque $x \notin \operatorname{ran} f_C$ y $x \notin \operatorname{ran} g_C$. Así, $\{\langle x, h(x)\rangle\}$ es aceptable y por lo tanto está incluida en $\bar{h}$. De aquí que $x \in \operatorname{dom}\bar{h}$. Esto muestra que $B \subseteq \operatorname{dom}\bar{h}$.

Afirmamos, además, que $\operatorname{dom}\bar{h}$ está cerrado bajo f y g. Para ello, consideremos cualesquiera s y t en $\operatorname{dom}\bar{h}$. Esperamos que $f(s,t) \in \operatorname{dom}\bar{h}$. Pero si no, entonces sea

$$v = \bar{h} \cup \{\langle f(s,t), F(\bar{h}(s),\bar{h}(t))\rangle\},$$

el resultado de agregar a $\bar{h}$ este par adicional. Está claro que v es una función, $\operatorname{dom} v \subseteq C$, y $\operatorname{ran} v \subseteq V$. Afirmamos que v satisface (i′) y (ii′).

Primero tomemos (i′). Si $x \in B \cap \operatorname{dom} v$, entonces $x \neq f(s,t)$, por libertad. De aquí que $x \in \operatorname{dom}\bar{h}$ y tenemos que $v(x) = \bar{h}(x) = h(x)$.

Ahora tomemos (ii′). Supongamos que $f(x,y) \in \operatorname{dom} v$ para algún x y algún y en C. Si $f(x,y) \in \operatorname{dom}\bar{h}$, entonces $v(f(x,y)) = \bar{h}(f(x,y)) = F(\bar{h}(x),\bar{h}(y)) = F(v(x), v(y))$, ya que $\bar{h}$ es aceptable. La otra posibilidad es que $f(x,y) = f(s,t)$. Entonces, por la libertad, tenemos que $x = s$ y $y = t$, y sabemos que estos puntos están en $\operatorname{dom}\bar{h} \subseteq \operatorname{dom} v$. Por construcción,

$$\begin{aligned} v(f(s,t)) &= F(\bar{h}(s),\bar{h}(t)) \\ &= F(v(s),v(t)). \end{aligned}$$

Finalmente, supongamos que $g(x) \in \operatorname{dom} v$ para x en C. Entonces, por la libertad tenemos que $g(x) \neq f(s,t)$. De

aquí que $g(x) \in \operatorname{dom}\overline{h}$, y en consecuencia $v(g(x)) = \overline{h}(g(x)) = G(\overline{h}(x)) = G(v(x))$.

Entonces v es aceptable. Pero eso nos dice que $v \subseteq \overline{h}$, así que finalmente $f(s,t) \in \operatorname{dom}\overline{h}$.

Un argumento similar muestra que $\operatorname{dom}\overline{h}$ también está cerrado bajo g. De aquí que $\operatorname{dom}\overline{h}$ sea inductivo y, por lo tanto, coincide con C.

4. Para mostrar que $\overline{h}$ es única, supongamos que $\overline{h}_1$ y $\overline{h}_2$ satisfacen ambas la conclusión del teorema. Sea S el conjunto sobre el cual coinciden:

$$S = \{x \in C \mid \overline{h}_1(x) = \overline{h}_2(x)\}.$$

Entonces no es difícil verificar que S es inductivo. En consecuencia, $S = C$ y $\overline{h}_1 = \overline{h}_2$. ⊣

Un comentario final sobre inducción y recursión: el principio de inducción que hemos enunciado no es el único posible. Es completamente posible dar demostraciones por inducción (y definiciones por recursión) sobre la longitud de las expresiones, el número de lugares en que ocurren símbolos de conectivo, etc. Estos métodos son inherentemente menos fundamentales, pero pueden ser necesarios en algunas situaciones.

Ejercicios

1. Supongamos que C está generado a partir de un conjunto $B = \{a, b\}$ por la operación binaria f y la operación unaria g. Enumere todos los elementos de C_2. ¿Cuántos elementos puede tener C_3? ¿Y C_4?

2. Evidentemente $(\mathbf{A}_3 \to \wedge \mathbf{A}_4)$ no es una fórmula. Demuéstrelo.

3. Podemos generalizar la discusión de esta sección pidiendo que $\mathcal{F}$ sea sólo una clase de relaciones en U. C_* se define como antes, excepto que $\langle x_0, x_1, \ldots, x_n\rangle$ es ahora una sucesión de construcción sii para cada $i \leq n$ tenemos o bien $x_i \in B$ o $\langle x_{j_1}, \ldots, x_{j_k}, x_i\rangle \in R$ para alguna $R \in \mathcal{F}$ y algunas $j_1, \ldots, j_k$, todas menores que i. Dé la definición correcta de C^* y pruebe que $C^* = C_*$.

5. *Conectivos de enunciado*

Hasta ahora hemos usado cinco símbolos de conectivo. Aun en ausencia de una definición general de "conectivo", está claro que los cinco conectivos que conocemos no son los únicos posibles. ¿Ganaríamos algo con aumentar conectivos al lenguaje? ¿Perderíamos algo omitiendo algunos de los conectivos que ya tenemos en el lenguaje?

En esta sección planteamos con mayor precisión estas preguntas y damos algunas respuestas. Primero consideremos un ejemplo informal. Podríamos expandir el lenguaje mediante un símbolo de conectivo de tres lugares, #, llamado símbolo de mayoría. Ahora permitimos que la expresión $(\#\alpha\beta\gamma)$ sea una fórmula cuando α, β y γ son fórmulas. En otras palabras, agregamos una sexta operación de construcción de fórmulas a nuestra lista:

$$\mathcal{E}_{\#}(\alpha,\beta,\gamma) = (\#\alpha\beta\gamma).$$

Ahora debemos dar la interpretación de este símbolo. Esto es, debemos decir cómo se calcula $\bar{v}((\#\alpha\beta\gamma))$ dados los valores $\bar{v}(\alpha)$, $\bar{v}(\beta)$ y $\bar{v}(\gamma)$. Elegimos la siguiente definición:

$\bar{v}((\#\alpha\beta\gamma))$ coincide con la mayoría de $\bar{v}(\alpha), \bar{v}(\beta)$ y $\bar{v}(\gamma)$.

Afirmamos que esta extensión no ha aportado nada en el siguiente sentido preciso: para toda fórmula del lenguaje extendido, existe en el lenguaje original una fórmula tautológicamente equivalente. (Por otro lado, la fórmula del lenguaje original puede ser mucho más larga que la fórmula del lenguaje extendido.) Probaremos esto (en una situación mucho más general) más adelante; aquí sólo haremos notar que se basa en el hecho de que $(\#\alpha\beta\gamma)$ es tautológicamente equivalente a:

$$(\alpha \wedge \beta) \vee (\alpha \wedge \gamma) \vee (\beta \wedge \gamma).$$

(Hacemos notar entre paréntesis que nuestra insistencia en que $\bar{v}((\#\alpha\beta\gamma))$ sea calculable a partir de $\langle\bar{v}(\alpha), \bar{v}(\beta), \bar{v}(\gamma)\rangle$ cumple aquí un papel definitivo. En el habla cotidiana hay operadores unarios como "es posible que" o "creo que". Podemos aplicar uno de estos operadores a un enunciado y producir otro enunciado cuya verdad o falsedad no se puede determinar

solamente con base en la verdad o la falsedad del enunciado original.)

Al generalizar el ejemplo anterior, el lenguaje formal será más un obstáculo que una ayuda. Podemos reformular el problema usando sólo funciones. Digamos que una ***función booleana*** de k lugares es una función de $\{F, V\}^k$ en $\{F, V\}$. (Una ***función booleana*** es, entonces, cualquier función booleana de k lugares para alguna k. Ampliamos esto un poco permitiendo que F y V sean funciones booleanas de cero lugares.) Como ejemplos de funciones booleanas tenemos las definidas por las siguientes ecuaciones (donde $X \in \{F, V\}$):

$$I_i^n(X_1, \ldots, X_n) = X_i,$$
$$N(F) = V, \quad N(V) = F,$$
$$K(V, V) = V, \quad K(F, X) = K(X, F) = F,$$
$$A(F, F) = F, \quad A(V, X) = A(X, V) = V,$$
$$C(V, F) = F, \quad C(F, X) = C(X, V) = V,$$
$$E(X, X) = V, \quad E(V, F) = E(F, V) = F.$$

A partir de una fórmula α podemos obtener una función booleana. Por ejemplo, si α es la fórmula $\mathbf{A}_1 \wedge \mathbf{A}_2$, entonces podemos hacer una tabla, la tabla V. Los 2^2 renglones de la tabla corresponden a las 2^2 asignaciones de verdad para $\{\mathbf{A}_1, \mathbf{A}_2\}$. Para cada una de las 2^2 parejas $\vec{X}$, hacemos $B_\alpha(\vec{X})$ igual al valor de verdad que α recibe cuando se da a sus símbolos de enunciado los valores indicados por $\vec{X}$.

Tabla V

$\mathbf{A}_1$	$\mathbf{A}_2$	$\mathbf{A}_1 \wedge \mathbf{A}_2$	
F	F	F	$B_\alpha(F, F) = F$
F	V	F	$B_\alpha(F, V) = F$
V	F	F	$B_\alpha(V, F) = F$
V	V	V	$B_\alpha(V, V) = V$

En general, supongamos que α es una fórmula cuyos símbolos de enunciado están entre $\mathbf{A}_1, \ldots, \mathbf{A}_n$. Definimos una fun-

ción booleana de n lugares B_α^n (o sólo B_α si n parece innecesario), la función booleana *realizada* por α, como

$$B_\alpha^n(X_1, \ldots, X_n) = \text{el valor que recibe } \alpha \text{ cuando a } \mathbf{A}_1, \ldots, \mathbf{A}_n \text{ se les dan los valores } X_1, \ldots, X_n.$$

En otras palabras: $B_\alpha^n(X_1, \ldots, X_n) = \bar{v}(\alpha)$, donde v es la asignación de verdad para $\{\mathbf{A}_1, \ldots, \mathbf{A}_n\}$ para la cual $v(\mathbf{A}_i) = X_i$. Así, B_α^n surge de considerar $\bar{v}(\alpha)$ como una función de v, con α fija.

Por ejemplo, las funciones booleanas mencionadas anteriormente se pueden obtener de esta manera:

$$I_i^n = B_{\mathbf{A}_i}^n,$$
$$N = B_{\neg \mathbf{A}_1}^1,$$
$$K = B_{\mathbf{A}_1 \wedge \mathbf{A}_2}^2,$$
$$A = B_{\mathbf{A}_1 \vee \mathbf{A}_2}^2,$$
$$C = B_{\mathbf{A}_1 \to \mathbf{A}_2}^2,$$
$$E = B_{\mathbf{A}_1 \leftrightarrow \mathbf{A}_2}^2.$$

A partir de estas funciones podemos componer otras. Por ejemplo:

$$B_{\neg \mathbf{A}_1 \vee \neg \mathbf{A}_2}^2(X_1, X_2) = A(N(I_1^2(X_1, X_2)), N(I_2^2(X_1, X_2))).$$

(El lado derecho de esta ecuación se puede comparar con el resultado de convertir $\neg \mathbf{A}_1 \vee \neg \mathbf{A}_2$ a notación polaca.) Dentro de poco llegaremos a la cuestión de si toda función booleana se puede obtener de esta manera.

Como afirma el teorema siguiente, al cambiar la atención de las fórmulas a las funciones booleanas que realizan, quedan identificadas entre sí las fórmulas tautológicamente equivalentes. Ordenemos el conjunto $\{F, V\}$ definiendo $F < V$. (Si $F = 0$ y $V = 1$, entonces éste es el orden natural.)

Teorema 15A Sean α y β fórmulas cuyos símbolos de enunciado están entre $\mathbf{A}_1, \ldots, \mathbf{A}_n$. Entonces

(a) $\alpha \models \beta$ sii para toda $\vec{X} \in \{F, V\}^n$, $B_\alpha(\vec{X}) \leq B_\beta(\vec{X})$.

(b) $\alpha \models\dashv \beta$ sii $B_\alpha = B_\beta$.

(c) $\models \alpha$ sii B_α es la función constante con valor V.

Demostración de (a) $\alpha \models \beta$ sii para todas las 2^n asignaciones de verdad v para $\mathbf{A}_1, \ldots, \mathbf{A}_n$ tales que $\bar{v}(\alpha) = V$, también $\bar{v}(\beta) = V$. (Esto es cierto aun si los símbolos de enunciado α y β no incluyen a todos los símbolos $\mathbf{A}_1, \ldots, \mathbf{A}_n$; *cfr.* el ejercicio 6 de la sección 2 de este capítulo.) Por tanto,

$\alpha \models \beta$ sii para todas las 2^n asignaciones v, $\quad \bar{v}(\alpha) = V \Rightarrow \bar{v}(\beta) = V$,

sii para todas las 2^n n-adas $\vec{X}$, $\quad B_\alpha^n(\vec{X}) = V \Rightarrow B_\beta^n(\vec{X}) = V$,

sii para todas las 2^n n-adas $\vec{X}$, $\quad B_\alpha^n(\vec{X}) \leq B_\beta^n(\vec{X})$,

donde $F < V$. ⊣

Además de identificar fórmulas tautológicamente equivalentes, nos hemos librado del lenguaje formal. Ahora estamos en libertad de considerar cualquier función booleana, sea o no realizada por alguna fórmula; aunque esta libertad es sólo aparente:

Teorema 15B Sea G una función booleana de n lugares, con $n \geq 1$. Podemos encontrar una fórmula α tal que $G = B_\alpha^n$, es decir, dicha α realiza la función G.

La razón principal de introducir funciones booleanas es poder formular este teorema, planteado por Emil Post en 1921.

Demostración Caso I: G es la función constante con valor F. Sea $\alpha = \mathbf{A}_1 \wedge \neg\mathbf{A}_1$.

Caso II: De otra forma, hay k puntos en los cuales G tiene el valor V, $k > 0$. Hagamos una lista de dichos puntos:

$$\vec{X}_1 = \langle X_{11}, X_{12}, \ldots, X_{1n}\rangle,$$
$$\vec{X}_2 = \langle X_{21}, X_{22}, \ldots, X_{2n}\rangle,$$
$$\ldots$$
$$\vec{X}_k = \langle X_{k1}, X_{k2}, \ldots, X_{kn}\rangle.$$

Sean

$$\beta_{ij} = \begin{cases} \mathbf{A}_j & \text{sii} \quad X_{ij} = V, \\ (\neg \mathbf{A}_j) & \text{sii} \quad X_{ij} = F, \end{cases}$$
$$\gamma_i = \beta_{i1} \wedge \cdots \wedge \beta_{in},$$
$$\alpha = \gamma_1 \vee \gamma_2 \vee \cdots \vee \gamma_k.$$

Afirmamos que $G = B^n_\alpha$.

En este momento podría ser de ayuda considerar un ejemplo concreto. Sea G la siguiente función booleana de tres lugares.

$$G(F, F, F) = F,$$
$$G(F, F, V) = V,$$
$$G(F, V, F) = V,$$
$$G(F, V, V) = F,$$
$$G(V, F, F) = V,$$
$$G(V, F, V) = F,$$
$$G(V, V, F) = F,$$
$$G(V, V, V) = V.$$

Entonces la lista de ternas en las cuales G toma el valor V tiene cuatro elementos:

$$\begin{array}{ll} FFV & \neg\mathbf{A}_1 \wedge \neg\mathbf{A}_2 \wedge \mathbf{A}_3, \\ FVF & \neg\mathbf{A}_1 \wedge \mathbf{A}_2 \wedge \neg\mathbf{A}_3, \\ VFF & \mathbf{A}_1 \wedge \neg\mathbf{A}_2 \wedge \neg\mathbf{A}_3, \\ VVV & \mathbf{A}_1 \wedge \mathbf{A}_2 \wedge \mathbf{A}_3. \end{array}$$

A la derecha de cada terna hemos escrito la conjunción correspondiente γ_i. Entonces α es la fórmula

$$(\neg\mathbf{A}_1 \wedge \neg\mathbf{A}_2 \wedge \mathbf{A}_3) \vee (\neg\mathbf{A}_1 \wedge \mathbf{A}_2 \wedge \neg\mathbf{A}_3) \vee$$
$$(\mathbf{A}_1 \wedge \neg\mathbf{A}_2 \wedge \neg\mathbf{A}_3) \vee (\mathbf{A}_1 \wedge \mathbf{A}_2 \wedge \mathbf{A}_3).$$

Nótese cómo α da una lista explícita de las ternas en las cuales G toma el valor V.

Para regresar a la demostración del teorema, nótese primero que $B^n_\alpha(\vec{X}_i) = V$ para $1 \leq i \leq k$. (Ya que la asignación de verdad correspondiente a $\vec{X}_i$ satisface γ_i y por

tanto satisface α.) Por otra parte, sólo una asignación de verdad para $\{A_1, \ldots, A_n\}$ puede satisfacer γ_i, de donde solamente k asignaciones tales pueden satisfacer α. Por tanto, $B^n_\alpha(\vec{Y}) = F$ para las demás $2^n - k$ n-adas $\vec{Y}$. Así, $B^n_\alpha(\vec{Y}) = G(\vec{Y})$ en todos los casos. ⊣

Con este teorema hemos averiguado que toda función booleana es realizable. Por supuesto que la α que realiza G no es única; cualquier fórmula tautológicamente equivalente también realizará la misma función. A veces es interesante escoger la α más breve posible. (En el ejemplo resuelto anteriormente, la fórmula

$$A_1 \leftrightarrow A_2 \leftrightarrow A_3$$

también realiza G.)

Como corolario del teorema anterior, podemos concluir que tenemos suficientes conectivos de enunciado (de hecho, más que suficientes). En efecto, supongamos que extendemos el lenguaje agregándole algunos exóticos conectivos nuevos (como el conectivo de mayoría discutido al principio de esta sección). Cualquier fórmula φ de este lenguaje extendido realiza alguna función booleana B^n_φ. Por el teorema anterior, tenemos una fórmula α del lenguaje original tal que $B^n_\varphi = B^n_\alpha$. Por tanto, φ y α son tautológicamente equivalentes, por el teorema 15A.

De hecho, la demostración prueba que α puede ser de cierta forma muy especial. Para empezar, los únicos conectivos de α son $\wedge$, $\vee$ y $\neg$. Además, α está en la llamada *forma normal disyuntiva* (abreviado: FND). Esto es, α es una disyunción

$$\alpha = \gamma_1 \vee \cdots \vee \gamma_k,$$

donde cada γ_i es una conjunción

$$\gamma_i = \beta_{i1} \wedge \cdots \wedge \beta_{in_i}$$

y cada β_{ij} es un símbolo de enunciado o la negación de un símbolo de enunciado. (Las ventajas de las fórmulas en forma normal disyuntiva surgen del hecho de que explícitamente listan las asignaciones de verdad que satisfacen la fórmula.) Tenemos entonces, como consecuencia:

Corolario 15C Para cualquier fórmula φ, podemos encontrar una fórmula tautológicamente equivalente α en forma normal disyuntiva.

Como toda función $G : \{F, V\}^n \rightarrow \{F, V\}$ para $n \geq 1$ puede ser realizada por una fórmula que usa sólo los símbolos de conectivo del conjunto $\{\wedge, \vee, \neg\}$, decimos que el conjunto $\{\wedge, \vee, \neg\}$ es *completo*. (En realidad, la completud es más una propiedad de las funciones booleanas K, A y N que corresponden a estos símbolos; pero la terminología anterior es conveniente.) Una vez que tenemos un conjunto completo de conectivos, sabemos que cualquier fórmula es tautológicamente equivalente a una fórmula cuyos conectivos están todos en dicho conjunto. (Pues dada cualquier fórmula φ, podemos hacer que α use dichos conectivos y que realice B_φ. Entonces $\alpha \models\models \varphi$.) La completud de $\{\wedge, \vee, \neg\}$ se puede mejorar:

Teorema 15D Tanto $\{\neg, \wedge\}$ como $\{\neg, \vee\}$ son completos.

Demostración Debemos probar que cualquier función booleana G puede ser realizada por una fórmula que use únicamente, en el primer caso, $\{\neg, \wedge\}$. Comenzamos por una fórmula α que use $\{\neg, \wedge, \vee\}$ y que realice G. Basta encontrar una fórmula tautológicamente equivalente α' que use solamente $\{\neg, \wedge\}$. Para esto usamos la ley de De Morgan:

$$\beta \vee \gamma \models\models \neg(\neg\beta \wedge \neg\gamma).$$

Aplicando repetidamente esta ley podemos eliminar por completo $\vee$ de α.

Más formalmente, podemos demostrar por inducción sobre α que existe una α' tautológicamente equivalente en la que sólo aparecen los conectivos $\wedge$, $\neg$. Los dos casos no triviales en el paso de inducción son:

Caso $\neg$: Si α es $(\neg\beta)$, hacemos α' igual a $(\neg\beta')$.

Caso $\vee$: Si α es $(\beta \vee \gamma)$, hacemos α' igual a $\neg(\neg\beta' \wedge \neg\gamma')$. Como β' y γ' son tautológicamente equivalentes a β y γ, respectivamente, entonces,

$$\begin{aligned}\alpha' &= \neg(\neg\beta' \wedge \neg\gamma')\\ &\models\!\!\dashv \neg(\neg\beta \wedge \neg\gamma)\\ &\models\!\!\dashv \beta \vee \gamma\\ &= \alpha.\end{aligned}$$

En demostraciones posteriores de que un conjunto de conectivos es completo, omitiremos esta inducción. Lo que haremos será, por ejemplo, dar solamente el método para simular $\vee$ usando $\neg$ y $\wedge$. ⊣

Demostrar que un conjunto dado de conectivos *no* es completo es generalmente más difícil que demostrar que uno es completo. El método básico consiste primero en demostrar (generalmente por inducción) que para toda fórmula α que use sólo esos conectivos, la función B^n_α tiene alguna peculiaridad, y después probar que alguna función booleana carece de dicha peculiaridad.

Ejemplo $\{\wedge, \rightarrow\}$ no es completo.

Demostración La idea es que con estos conectivos, si se asigna V a los símbolos de enunciado, entonces toda la fórmula recibe el valor V. En particular, no se obtiene nada tautológicamente equivalente a $\neg\mathbf{A}$.

Más detalladamente, podemos probar por inducción que para cualquier fórmula α que use sólo estos conectivos y que tenga **A** como único símbolo de enunciado, tenemos que $\mathbf{A} \models \alpha$. (En términos de funciones, esto afirma que $B^1_\alpha(V) = V$.) El mismo argumento prueba que $\{\wedge, \vee, \rightarrow, \leftrightarrow\}$ no es completo. ⊣

Para cada n existen 2^{2^n} funciones booleanas de n variables. Por tanto, si identificamos cada conectivo con su función booleana (por ejemplo, $\wedge$ con la función K mencionada anteriormente), tenemos que hay 2^{2^n} conectivos n-arios. Ahora los catalogaremos para $n \leq 2$.

Conectivos ceroarios

Hay dos funciones booleanas de cero variables, F y V. Como símbolos de conectivo correspondientes tomamos $\bot$ y $\top$. Ahora, un conectivo n-ario se combina con n fórmulas para produ-

cir una nueva fórmula. Cuando $n = 0$, tenemos que $\bot$ es por sí mismo una fórmula. Difiere de los símbolos de enunciado en que $\bar{v}(\bot) = F$ para toda v; es decir, $\bot$ es un símbolo lógico al que siempre se le asigna el valor F. De igual forma, $\top$ es una fórmula, y $\bar{v}(\top) = V$ para toda v. Entonces, por ejemplo, $\mathbf{A} \rightarrow \bot$ es una fórmula, tautológicamente equivalente a $\neg \mathbf{A}$, como puede verse con una tabla de verdad de dos renglones.

Conectivos unarios

Hay cuatro conectivos unarios, pero sólo uno de interés. El caso interesante es la negación. Las otras tres funciones booleanas de un lugar son la función identidad y las dos funciones constantes.

Conectivos binarios

Hay dieciséis conectivos binarios, pero sólo los últimos diez que aparecen en la tabla VI de la página siguiente son "realmente binarios".

Conectivos ternarios

Hay 256 conectivos ternarios; dos de ellos son esencialmente ceroarios, 6 $(= 2 \cdot \binom{3}{1})$ son esencialmente unarios, y $30 (= 10 \cdot \binom{3}{2})$ son esencialmente binarios. Esto nos deja con 218 que son realmente ternarios. Hasta ahora sólo hemos mencionado el conectivo de mayoría $\#$. Está, de igual forma, el conectivo de minoría. En el ejercicio 7 encontraremos $+^3$, la suma ternaria módulo 2. A $+^3\ \alpha\beta\gamma$ se le asigna el valor V sii un número impar de las fórmulas α, β y γ tienen el valor V. Esta fórmula es equivalente tanto a $\alpha + \beta + \gamma$ como a $\alpha \leftrightarrow \beta \leftrightarrow \gamma$. En el ejercicio 8 encontraremos otro conectivo ternario.

Ejemplo $\{|\}$ y $\{\downarrow\}$ son completos.

Demostración Para $|$:

$$\neg\alpha \models\!\!\dashv \alpha \,|\, \alpha$$
$$\alpha \vee \beta \models\!\!\dashv (\neg\alpha)|(\neg\beta).$$

Como $\{\neg, \vee\}$ es completo y se pueden simular $\neg$, $\vee$ usando solamente $|$, entonces $\{|\}$ es completo. $\dashv$

Tabla VI

Símbolo	Equivalente	Observaciones
	$\top$	constante de dos variables, esencialmente ceroario
	$\bot$	constante de dos variables, esencialmente ceroario
	A	proyección, esencialmente unario
	B	proyección, esencialmente unario
	$\neg$**A**	negación, esencialmente unario
	$\neg$**B**	negación, esencialmente unario
$\wedge$	**A** $\wedge$ **B**	y; si $F = 0$ y $V = 1$, entonces ésta es la multiplicación en el campo $\{0, 1\}$
$\vee$	**A** $\vee$ **B**	o (inclusivo)
$\rightarrow$	**A** $\rightarrow$ **B**	condicional
$\leftrightarrow$	**A** $\leftrightarrow$ **B**	bicondicional
$\leftarrow$	**A** $\leftarrow$ **B**	condicional invertido
$+$	(**A** $\vee$ **B**) $\wedge$ $\neg$(**A** $\wedge$ **B**)	o exclusivo, "**A** o **B** pero no ambas"; si $F = 0$ y $V = 1$, entonces ésta es la suma usual (módulo 2) en el campo $\{0, 1\}$
$\downarrow$	$\neg$(**A** $\vee$ **B**)	nor, "ni **A** ni **B**"
$\mid$	$\neg$(**A** $\wedge$ **B**)	nand, "no ambas **A** y **B**"; el símbolo se llama raya de Sheffer
$<$	($\neg$**A**) $\wedge$ **B**	el orden usual, donde $F < V$
$>$	**A** $\wedge$ ($\neg$**B**)	el orden usual, donde $F < V$

EJEMPLO $\{\neg, \rightarrow\}$ es completo. De hecho, de los diez conectivos que son realmente binarios, ocho tienen la propiedad de formar, cuando se agregan a $\neg$, un conjunto completo. Las dos excepciones son $+$ y $\leftrightarrow$; véase el ejercicio 5.

EJEMPLO $\{\bot, \rightarrow\}$ es completo. De hecho, como con este conjunto podemos realizar incluso las dos funciones booleanas ceroarias, es supercompleto.

Ejercicios

1. Sea G la siguiente función booleana de tres lugares.

$$\begin{array}{ll} G(F,F,F) = V, & G(V,F,F) = V, \\ G(F,F,V) = V, & G(V,F,V) = F, \\ G(F,V,F) = V, & G(V,V,F) = F, \\ G(F,V,V) = F, & G(V,V,V) = F. \end{array}$$

   (a) Encuentre una fórmula que use a lo sumo los conectivos $\vee$, $\wedge$ y $\neg$, tal que realice G.

   (b) Luego encuentre una fórmula en que los símbolos de conectivo aparezcan en no más de cinco lugares.

2. Pruebe que $|$ y $\downarrow$ son los únicos conectivos binarios completos por sí mismos.

3. Pruebe que $\{\neg, \#\}$ no es completo.

4. Sea M el conectivo ternario de minoría. (Así, $\bar{v}(\mathrm{M}\alpha\beta\gamma)$ siempre difiere de la mayoría de $\bar{v}(\alpha)$, $\bar{v}(\beta)$ y $\bar{v}(\gamma)$.) Pruebe lo siguiente:

   (a) $\{\mathrm{M}, \bot\}$ es completo.

   (b) $\{\mathrm{M}\}$ no es completo.

5. Pruebe que $\{\top, \bot, \neg, \leftrightarrow, +\}$ no es completo. *Sugerencia:* Pruebe que cualquier fórmula α que use sólo estos conectivos y los símbolos de enunciado **A** y **B** tiene un número par de valores de verdad V entre los cuatro valores posibles de $\bar{v}(\alpha)$.

   Observación: Otro enfoque usa el álgebra del campo $\{0, 1\}$. Cualquier función booleana realizable con estos conectivos tiene cierta propiedad de linealidad.

6. Pruebe que $\{\wedge, \leftrightarrow, +\}$ es completo pero que ningún subconjunto propio es completo.

7. Sea $+^3$ el conectivo ternario tal que $+^3\alpha\beta\gamma$ es equivalente a $\alpha + \beta + \gamma$.

   (a) Pruebe que $\{\top, \bot, \wedge, +^3\}$ es completo.

   (b) Pruebe que ningún subconjunto propio es completo.

Observación: $+^3$ es el conectivo ternario de *paridad*; la condición para que $\bar{v}(+\ \alpha_1\alpha_2\alpha_3) = V$ es que $\bar{v}(\alpha_i) = V$ para un número *impar* de i's. $+$ es el conectivo binario de paridad. La función G en la prueba del teorema 15B es la función de paridad de tres lugares.

8. Sea $\mathbb{I}$ el conectivo ternario tal que $\mathbb{I}\alpha\beta\gamma$ recibe el valor V sii exactamente a una de las fórmulas α, β, γ se le asigna el valor V. Pruebe que no existen conectivos binarios $\circ$ y $\triangle$ tales que $\mathbb{I}\alpha\beta\gamma$ es equivalente a $(\alpha \circ \beta) \triangle \gamma$.

9. Decimos que una fórmula α está en *forma normal conjuntiva* (abreviado: FNC) sii es una conjunción

$$\alpha = \gamma_1 \wedge \cdots \wedge \gamma_k$$

donde cada γ_i es una disyunción

$$\gamma_i = \beta_{i1} \vee \cdots \vee \beta_{in}$$

y cada β_{ij} es o un símbolo de enunciado, o la negación de un símbolo de enunciado.

(a) Encuentre una fórmula en forma normal conjuntiva que sea tautológicamente equivalente a $\mathbf{A} \leftrightarrow \mathbf{B} \leftrightarrow \mathbf{C}$.

(b) Pruebe que para cualquier fórmula podemos encontrar una fórmula tautológicamente equivalente en forma normal conjuntiva.

10. Agregamos los conectivos ceroarios $\top$, $\perp$ a nuestro lenguaje. Para cada fórmula φ y cada símbolo de enunciado A, sea $\varphi^A_\top$ la fórmula que se obtiene de φ reemplazando A por $\top$. De igual forma para $\varphi^A_\perp$. Entonces sea $\varphi^A_* = (\varphi^A_\top \vee \varphi^A_\perp)$. Pruebe lo siguiente:

(a) $\varphi \models \varphi^A_*$.

(b) Si $\varphi \models \psi$ y A no aparece en ψ, entonces $\varphi^A_* \models \psi$.

(c) La fórmula φ es satisfactible sii φ^A_* es satisfactible.

Observaciones: Podemos pensar que φ^A_* trata de decir todo lo que dice φ, pero sin poder usar el símbolo A. Las partes (a) y (b) expresan que φ^A_* es la consecuencia,

libre de A, más fuerte de φ. Las fórmulas φ y φ_*^A no son en general tautológicamente equivalentes, pero son "igualmente satisfactibles" por la parte (c). La operación de construir φ_*^A a partir de φ se llama (en otro contexto) *resolución* en A.

11. (Teorema de interpolación.) Si $\alpha \models \beta$, entonces existe alguna γ cuyos símbolos de enunciado aparecen todos tanto en α como en β, y tal que $\alpha \models \gamma \models \beta$. *Sugerencia:* use el ejercicio anterior.

    Observaciones: Hay un análogo del ejercicio 11 que se cumple para la lógica de primer orden; pero la prueba en ese caso es muy diferente, porque no hay un análogo del ejercicio 10.

12. ¿Es completo el conjunto $\{\wedge, \top, \bot\}$? Justifique su respuesta.

6. *Circuitos digitales*[4]

Consideremos un dispositivo eléctrico (tradicionalmente una caja negra) con n entradas y una salida (Fig. 1). Supongamos que a cada entrada le aplicamos una señal con uno de dos valores y que la salida tiene uno de dos valores. Llamamos a los dos valores posibles F y V. (También podríamos definir el valor F como potencial 0 y escoger la unidad de potencial de tal manera que el valor V tenga potencial 1.) Supongamos, además, que el dispositivo no tiene memoria; es decir, el nivel actual de la salida depende solamente de las entradas actuales (y no de la historia pasada). Entonces el funcionamiento del dispositivo queda descrito por una función booleana:

$$G(X_1, \ldots, X_n) = \text{el nivel de salida dadas las señales de entrada } X_1, \ldots, X_n.$$

El estudio de dispositivos que satisfacen todas estas suposiciones constituye una parte esencial de la teoría de circuitos

[4] Es posible omitir esta sección, que discute una aplicación de las ideas de las secciones anteriores, sin pérdida de continuidad.

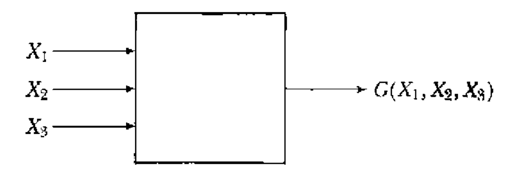


FIGURA 1. *Dispositivo eléctrico con tres entradas*

de computadoras digitales. Existe, por ejemplo, la compuerta AND de dos entradas, para la cual la salida es el mínimo de las entradas (donde $F < V$). Este dispositivo realiza la función booleana K de la sección precedente. Es conveniente asignar las etiquetas $\mathbf{A}_1$ y $\mathbf{A}_2$ a las entradas y la etiqueta $\mathbf{A}_1 \wedge \mathbf{A}_2$ a la salida.

Se pueden hacer dispositivos semejantes para otros conectivos. Para una compuerta OR de dos entradas (Fig. 2, p. 87), el voltaje de salida es el máximo de los voltajes de entrada. El correspondiente al conectivo de negación es el dispositivo NOT (o inversor), cuyo voltaje de salida es el opuesto al voltaje de entrada.

A partir de varios dispositivos de este tipo se puede construir un circuito, y de nuevo es natural usar fórmulas de nuestro lenguaje formal para etiquetar los voltajes en diferentes puntos (Fig. 3, p. 87). Inversamente, dada la fórmula asociada de esta manera a la salida, podemos reconstruir aproximadamente el circuito, que se parece mucho al árbol de construcción de la fórmula.

Por ejemplo, el circuito correspondiente a

$$((\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{D}) \vee ((\mathbf{A} \wedge \mathbf{B}) \wedge \neg \mathbf{C})$$

probablemente sería el mostrado en la figura 4 (p. 87). Por lo general, la duplicación del circuito correspondiente a $\mathbf{A} \wedge \mathbf{B}$ no sería deseable.

Fórmulas tautológicamente equivalentes entre sí dan lugar a circuitos fundamentalmente con el mismo comportamiento, aunque posiblemente a distinto costo y (si los dispositivos no son de operación instantánea) a distinta velocidad. Definamos

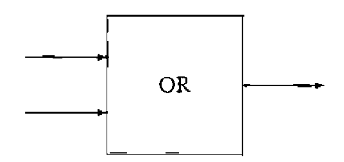


FIGURA 2. *Compuerta OR*

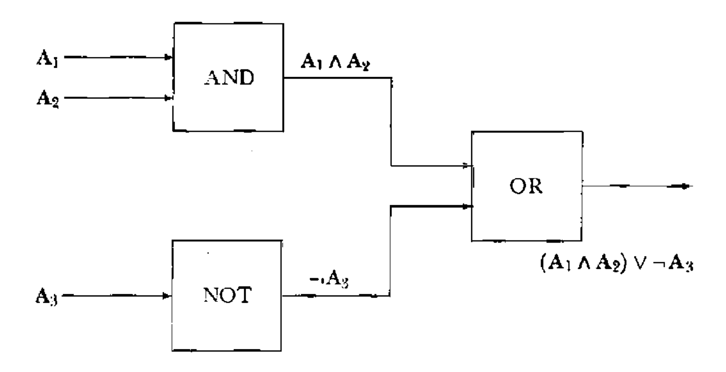


FIGURA 3. *Circuito etiquetado con fórmulas*

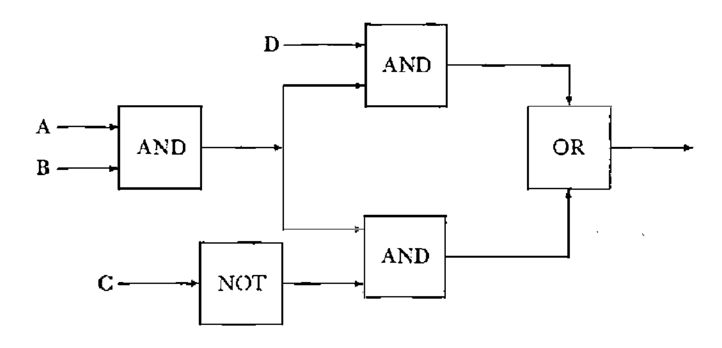


FIGURA 4. *Circuito correspondiente a* $((A \wedge B) \wedge D) \vee ((A \wedge B) \wedge \neg C)$

el *retraso* de un circuito (también llamado la *profundidad*) como el máximo número de cajas a través de las cuales puede pasar la señal al ir de una entrada a la salida. La noción correspondiente para fórmulas se define convenientemente por recursión.

1. El retraso de un símbolo de enunciado es 0.
2. El retraso de $\neg\alpha$ es igual a uno más el retraso de α.
3. El retraso de $\alpha \wedge \beta$ es igual a uno más el máximo del retraso de α y el retraso de β.

Y de forma similar para los demás conectivos.

Por ejemplo, el circuito de $(A_1 \wedge A_2) \vee \neg A_3$ usa tres dispositivos y tiene un retraso igual a 2. La fórmula tautológicamente equivalente $\neg(A_3 \wedge (\neg A_1 \vee \neg A_2))$ da lugar a un circuito con cinco dispositivos y un retraso igual a 4. El problema que enfrentan muchos ingenieros en computación es el siguiente: dado un circuito (o su fórmula correspondiente), encontrar un circuito equivalente (o una fórmula tautológicamente equivalente) para el cual el costo sea mínimo, sujeto a restricciones tales como máximo retraso permisible. Para este problema se cuenta con un catálogo de dispositivos que se pueden usar; por ejemplo:

NOT, AND de dos entradas, OR de tres entradas.

(Es claramente deseable que los dispositivos disponibles correspondan a un conjunto completo de conectivos.) El catálogo de dispositivos determina un lenguaje formal, con un conectivo para cada dispositivo.

Ejemplo 1 Entradas A, B, C. Salida: que coincida con la mayoría de A, B y C. Dispositivos disponibles: OR de dos entradas, AND de dos entradas. Una solución es:

$$((A \wedge B) \vee (A \wedge C)) \vee (B \wedge C),$$

que usa cinco dispositivos y tiene un retraso de 3. Pero una mejor solución es:

$$(A \wedge (B \vee C)) \vee (B \wedge C),$$

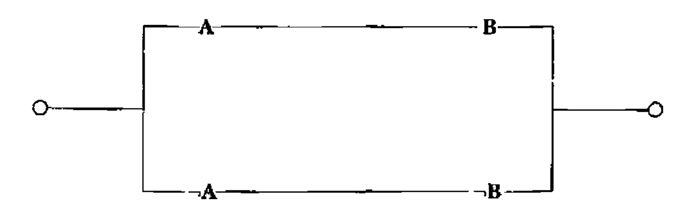


FIGURA 5. *Diagrama de alambrado para* (A∧ B) ∨ (¬ A ∧ ¬ B)

que usa cuatro dispositivos y tiene el mismo retraso. Lo que es más, no hay solución que use solamente tres dispositivos; *cfr.* el ejercicio 1.

EJEMPLO 2 Entradas: **A** y **B**. Salida: *V* si las entradas coinciden, *F* si no coinciden; es decir, el circuito examina la igualdad de las entradas. Dispositivo disponible: NOR de dos entradas. Una solución es:

$$((\mathbf{A} \downarrow \mathbf{A}) \downarrow \mathbf{B}) \downarrow ((\mathbf{B} \downarrow \mathbf{B}) \downarrow \mathbf{A}).$$

Esto usa cinco dispositivos; ¿existe una solución mejor? Una pregunta más profunda es: ¿existe algún procedimiento eficiente para encontrar una solución minimal? Aquí solo planteamos estas preguntas. En años recientes se ha trabajado mucho en la investigación de cuestiones de este tipo.

EJEMPLO 3 (Circuitos de relevadores.) Entradas: **A**, ¬**A**, **B**, ¬ **B**, . . . Dispositivos: OR (cualquier número de entradas), AND (cualquier número de entradas). Costo: los dispositivos son gratis, pero cada uso de una entrada cuesta una unidad. Para verificar la igualdad de **A** y **B** podríamos usar:

$$(\mathbf{A} \wedge \mathbf{B}) \vee (\neg \mathbf{A} \wedge \neg \mathbf{B}).$$

El diagrama de alambrado para el circuito aparece en la figura 5. El circuito deja pasar corriente sii **A** y **B** tienen el mismo valor. (Esta fórmula, equivalente a **A** ↔ **B**, tiene la propiedad de que su valor de verdad cambia cuan-

do cambia el valor de verdad de alguno de sus argumentos. Por esta razón, el circuito se usa, con interruptores dobles, en el alambrado de iluminación de corredores.)

Pero hay un aspecto en el que los circuitos de relevadores no satisfacen la descripción dada al comienzo de la presente sección. Los relevadores son dispositivos bilaterales; dejan pasar corriente en cualquier dirección. Esta característica hace posibles los circuitos "puente" (Fig. 6, p. 91). Los métodos descritos aquí no se aplican a tales circuitos.

EJEMPLO 4 Hay cuatro entradas, y el circuito debe realizar la función booleana G, donde G toma el valor V en los puntos $\langle F, F, F, V\rangle$, $\langle F, F, V, F\rangle$, $\langle F, F, V, V\rangle$, $\langle F, V, F, F\rangle$, $\langle F, V, F, V\rangle$, $\langle F, V, V, F\rangle$, $\langle F, V, V, V\rangle$ y $\langle V, F, F, V\rangle$. G toma el valor F en los puntos $\langle V, F, F, F\rangle$, $\langle V, F, V, F\rangle$, $\langle V, V, F, F\rangle$, $\langle V, V, V, F\rangle$ y $\langle V, V, V, V\rangle$. En los tres puntos restantes, $\langle F, F, F, F\rangle$, $\langle V, F, V, V\rangle$ y $\langle V, V, F, V\rangle$, no nos interesa el valor de G. (La aplicación del circuito es tal que estas tres combinaciones nunca ocurren.)

Sabemos que G se puede realizar usando, digamos $\{\wedge, \vee, \neg\}$; pero queremos hacer esto de manera eficiente. El primer paso consiste en representar los datos de una manera más comprensible. Podemos hacer esto por medio de la figura 7 (p. 91). Como $G(F, F, F, V) = V$, hemos colocado una V en el cuadro de coordenadas $\langle \neg\mathbf{A}, \neg\mathbf{B}, \neg\mathbf{C}, \mathbf{D}\rangle$. De forma análoga, hay una F en el cuadrado de coordenadas $\langle \mathbf{A}, \mathbf{B}, \neg\mathbf{C}, \neg\mathbf{D}\rangle$ porque $G(V, V, F, F) = F$. Los tres cuadrados que no nos interesan se han quedado en blanco.

Ahora buscamos un patrón geométrico sencillo. El área gris incluye todas las V y ninguna F. Corresponde a la fórmula

$$(\neg\mathbf{A}) \vee (\neg\mathbf{C} \wedge \mathbf{D}),$$

que es razonablemente sencilla y satisface todas nuestras condiciones. Nótese que la entrada **B** no se necesita.

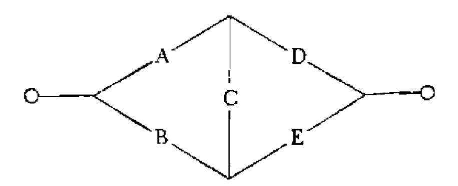


FIGURA 6. *Circuito puente*

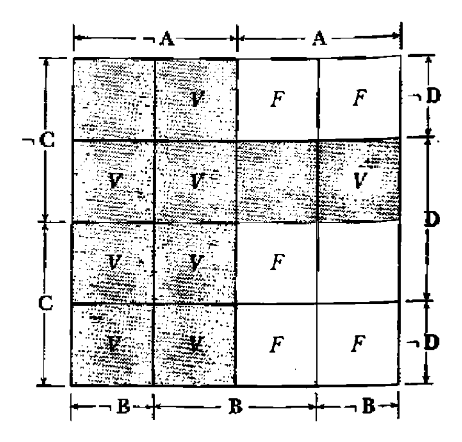


FIGURA 7. *Diagrama para el ejemplo 4*

Ejercicios

1. En el ejemplo 1 de esta sección, verifique que no existe ninguna solución que use solamente tres dispositivos.

2. Definamos una *literal* como una fórmula que es o bien un símbolo de enunciado o la negación de un símbolo de enunciado. Un *implicante* de φ es una conjunción α de literales (con distintos símbolos de enunciado) tal que $\alpha \models \varphi$. En la sección 5 de este capítulo (*cfr.* corolario 15C) probamos que toda fórmula satisfactible φ es tautológicamente equivalente a una disyunción $\alpha_1 \vee \cdots \vee \alpha_n$ donde

cada α_i es un implicante de φ. Un implicante α de φ es *primo* sii deja de ser un implicante al borrar cualquiera de sus literales. Cualquier disyunción de implicantes equivalente a φ, de longitud mínima, debe estar constituida únicamente por implicantes primos.

(a) Encuentre todos los implicantes primos de

$$(\mathbf{A} \to \mathbf{B}) \wedge (\neg A \to \mathbf{C}).$$

(b) ¿Cuáles disyunciones de implicantes primos tienen la propiedad de ser tautológicamente equivalentes a la fórmula de la parte (a)?

3. Repita (a) y (b) del ejercicio 2, pero para la fórmula

$$(\mathbf{A} \vee \neg \mathbf{B}) \wedge (\neg \mathbf{C} \vee \mathbf{D}) \to \mathbf{B} \wedge ((\mathbf{A} \wedge \mathbf{C}) \vee (\neg \mathbf{C} \wedge \mathbf{D})).$$

7. *Compacidad y efectividad*

Compacidad

Ahora daremos una demostración del teorema de compacidad mencionado anteriormente (Sec. 2). Llamemos *satisfactible* a un conjunto Σ de fórmulas sii existe una asignación de verdad que satisface a todos los elementos de Σ.

Teorema de compacidad Un conjunto de fórmulas es satisfactible sii todos sus subconjuntos finitos son satisfactibles.

Por el momento digamos que Σ es *finitamente satisfactible* sii todo subconjunto finito de Σ es satisfactible. Entonces el teorema de compacidad afirma que esta noción coincide con la de satisfactibilidad. Nótese que si Σ es satisfactible, entonces automáticamente es finitamente satisfactible. También si Σ es finito, entonces la inversa es trivial. (Todo conjunto es un subconjunto de sí mismo.) La parte no trivial consiste en probar que si un conjunto infinito es finitamente satisfactible, entonces es satisfactible.

Demostración del teorema de compacidad La demostración consta de dos partes. En la primera parte tomamos nuestro conjunto finitamente satisfactible Σ y lo extendemos a

un conjunto finitamente satisfactible maximal Δ. En la segunda parte usamos Δ para construir una asignación de verdad que satisfaga a Σ.

Para la primera parte sea $\alpha_1, \alpha_2 \ldots$ una enumeración fija de las fórmulas. (Esto es posible porque el conjunto de los símbolos de enunciado, y por tanto el de las expresiones, es numerable; véase el teorema 0B). Definamos por recursión (sobre los números naturales)

$$\Delta_0 = \Sigma,$$

$$\Delta_{n+1} = \begin{cases} \Delta_n;\ \alpha_{n+1} & \text{si esto es finitamente satisfactible,} \\ \Delta_n;\ \neg\alpha_{n+1} & \text{en otro caso.} \end{cases}$$

(Recordemos que $\Delta_n;\ \alpha_{n+1} = \Delta_n \cup \{\alpha_{n+1}\}$.) Por tanto, cada Δ_n es finitamente satisfactible; véase el ejercicio 1.) Sea $\Delta = \bigcup_n \Delta_n$, el límite de las Δ_n.

Queda claro que (1) $\Sigma \subseteq \Delta$ y que (2) para toda fórmula α o bien $\alpha \in \Delta$, o bien $(\neg\alpha) \in \Delta$. Además, (3) Δ es finitamente satisfactible, puesto que todo subconjunto finito de Δ es ya un subconjunto finito de alguna Δ_n y es, por tanto, satisfactible.

Esto concluye la primera parte de la demostración; ahora tenemos un conjunto Δ con las propiedades (1)–(3). En general, tal conjunto no es único, pero al menos existe uno. (Una demostración alternativa de la existencia de tal Δ —demostración que podríamos usar aun cuando hubiera una cantidad no numerable de símbolos de enunciado— emplea el lema de Zorn. El lector familiarizado con los usos del lema de Zorn debería percibir su aplicabilidad en el presente caso.)

Para la segunda parte de la prueba definimos una asignación de verdad v para el conjunto de todos los símbolos de enunciado:

$$v(A) = V \quad \text{sii} \quad A \in \Delta$$

para cualquier símbolo de enunciado A. Entonces, tenemos que para toda fórmula φ,

$$v \text{ satisface } \varphi \quad \text{sii} \quad \varphi \in \Delta.$$

Esto se demuestra por inducción sobre φ; véase el ejercicio 2. Como $\Sigma \subseteq \Delta$, v debe entonces satisfacer todos los elementos de Σ. ⊣

Corolario 17A Si $\Sigma \models \tau$, entonces existe un subconjunto finito $\Sigma_0 \subseteq \Sigma$ tal que $\Sigma_0 \models \tau$.

Demostración Hacemos uso del hecho elemental de que $\Sigma \models \tau$ sii $\Sigma; \neg\tau$ es insatisfactible.

$\Sigma_0 \not\models \tau$ para todo conjunto finito $\Sigma_0 \subseteq \Sigma$

$\Rightarrow \Sigma_0; \neg\tau$ es satisfactible para cualquier conjunto finito$\Sigma_0 \subseteq \Sigma$

$\Rightarrow \Sigma; \neg\tau$ es finitamente satisfactible

$\Rightarrow \Sigma; \neg\tau$ es satisfactible

$\Rightarrow \Sigma \not\models \tau$. ⊣

En realidad, el corolario anterior es equivalente al teorema de compacidad; véase el ejercicio 3.

Efectividad y calculabilidad

Aunque el método de tablas de verdad es bastante engorroso de usar, la existencia del método tiene conclusiones teóricas interesantes. Supóngase que nos preguntamos acerca de un conjunto Σ de fórmulas si existe un procedimiento *efectivo* que, dada una fórmula τ, decida si $\Sigma \models \tau$ o si no. Entiendo por procedimiento efectivo el que satisface las siguientes condiciones:

1. Debe haber instrucciones exactas (es decir, un *programa*) que expliquen cómo ejecutar el procedimiento. Las instrucciones deben ser de longitud finita. Después de todo, tiene que ser posible *dar* las instrucciones a la persona o máquina encargada de hacer los cálculos, y no podemos dar a alguien todo lo que hay en un objeto infinito. Sin embargo, de antemano nos abstenemos de imponer un límite superior a la longitud de las instrucciones. Si hay más líneas en las instrucciones que electrones en el universo, solamente alzamos los hombros y decimos: "Ése es un programa bastante largo."

2. Estas instrucciones no deben exigir ni ingenio ni originalidad de parte de la persona o la máquina que haya de seguir-

las. La idea es que un empleado diligente (que no sepa matemáticas pero que sea muy bueno para seguir instrucciones) o nuestra computadora (que no piensa) sean capaces de ejecutar las instrucciones. Es decir, debe ser posible que las instrucciones *se implementen mecánicamente*. El procedimiento debe evitar medios aleatorios (como lanzar una moneda) o cualquier otro recurso que, en la práctica, sólo sea aproximado.

3. En el caso de un procedimiento de decisión, como el mencionado anteriormente, el procedimiento debe ser tal que, dada una fórmula τ, produzca una respuesta afirmativa o negativa después de un número finito de pasos. (Es decir, el procedimiento debe ser un *algoritmo* para determinar la respuesta.)

Por otro lado, no ponemos anticipadamente ninguna cota en la cantidad de tiempo que podría requerirse antes de que aparezca la respuesta. Tampoco ponemos de antemano ninguna cota en la cantidad de papel (o de algún otro medio de almacenamiento) que se pueda requerir. Todo esto dependerá, entre otras cosas, de la entrada τ. Pero, para cualquier τ, el procedimiento debe exigir sólo un número finito de pasos para producir la respuesta, y por tanto sólo consumirá una cantidad finita de papel. No se vale realizar un número infinito de pasos y *después* dar la respuesta.

La gente que usa computadoras digitales puede considerar que un procedimiento es efectivo sólo cuando su máquina lo puede llevar a cabo en un tiempo "razonable". Desde luego, el tiempo razonable puede cambiar según las circunstancias; tal vez esa gente planee comprar una máquina más rápida y con más memoria el año siguiente; para entonces, su idea de lo que pueda hacerse en un tiempo razonable aumentará considerablemente. Lo que aquí queremos es un concepto de procedimiento efectivo que sea el caso ideal donde se eliminen todas las restricciones prácticas acerca del tiempo de proceso y del espacio de memoria.

Por supuesto que la descripción anterior difícilmente puede considerarse una definición precisa de la palabra "efectivo"; de hecho, en este libro usaremos esta palabra solamente de una manera informal e intuitiva. (En el capítulo III encontraremos una contrapartida precisa, el concepto de "recursivo".)

Pero mientras nos restrinjamos a afirmaciones positivas de que *sí* existe un procedimiento efectivo de cierto tipo, basta el punto de vista intuitivo. Simplemente hacemos uso del procedimiento, probamos que sirve, y las demás personas estarán de acuerdo en que es efectivo. (Pero esto descansa sobre el hecho *empírico* de que los procedimientos que a un matemático le parecen efectivos también le parecen así a otros.) Si quisiéramos un resultado negativo, de que *no* existe un procedimiento efectivo de cierto tipo, entonces este punto de vista intuitivo no sería adecuado. (En el capítulo III sí necesitaremos obtener precisamente tales resultados negativos.) Como la noción de efectividad es intuitiva, señalaremos con un asterisco las definiciones y teoremas que la involucren. Por ejemplo:

*Teorema 17B Existe un procedimiento efectivo que, dada cualquier expresión ε, decide si es una fórmula o no lo es.

Demostración Véanse el algoritmo de la sección 3 de este capítulo y las notas correspondientes. ⊣

Aquí hay una cuestión técnica que surge del hecho de que nuestro lenguaje tiene una infinidad de símbolos de enunciado diferentes. Cuando hablamos de que una expresión ε está "dada", nos imaginamos que alguien pudiera poner por escrito los símbolos de ε, uno tras otro. Resulta inverosímil que alguien tenga la capacidad para escribir todos y cada uno de esa infinitud de símbolos. Para evitar esto, adoptamos el siguiente "formato de entrada/salida": en lugar de escribir A_5, por ejemplo, usamos A'''', una cadena de cinco símbolos. Ahora el número total de símbolos en nuestro alfabeto es sólo de nueve:

$$(,\ ),\ \neg,\ \wedge,\ \vee,\ \rightarrow,\ \leftrightarrow,\ A,\ \text{y}\ '.$$

(Si identificamos estos nueve símbolos con los dígitos 1–9, ¡obtendremos expresiones que lucen particularmente conocidas en entornos computacionales! Y todavía tenemos el dígito 0 para separar expresiones.)

El teorema 17B afirma que el conjunto de todas las fórmulas es *decidible* en el sentido de la siguiente definición:

Definición Un conjunto Σ de expresiones es ***decidible*** sii existe un procedimiento efectivo que, dada una expresión α, decida si $\alpha \in \Sigma$ o no.

Por ejemplo, todo conjunto finito es decidible. (Las instrucciones pueden simplemente listar el número finito de elementos del conjunto; entonces el algoritmo puede cotejar la entrada con la lista.) Algunos conjuntos infinitos son decidibles, pero no todos. Por un lado, hay un número incontable ($2^{\aleph_0}$, para ser exactos) de conjuntos de expresiones. Por otro, sólo puede haber un número contable de procedimientos efectivos. Esto es así porque un procedimiento está completamente determinado por sus instrucciones (finitas). Solamente hay $\aleph_0$ sucesiones finitas de letras, y las instrucciones, al ponerlas por escrito, constituyen una sucesión finita de letras.

***Teorema 17C** Hay un procedimiento efectivo que, dado un conjunto finito $\Sigma; \tau$ de fórmulas, decide si $\Sigma \models \tau$ o no.

Demostración El procedimiento de tablas de verdad (sección 2 de este capítulo) cumple con lo requerido. ⊣

En este teorema hemos especificado la finitud de $\Sigma; \tau$, ya que no se puede "dar" de manera directa o efectiva la totalidad de un objeto infinito.

***Corolario 17D** Dado un conjunto finito Σ, el conjunto de las consecuencias tautológicas de Σ es decidible. En particular, es decidible el conjunto de las tautologías.

Si Σ es un conjunto infinito —aún uno decidible—, entonces, por lo general, el conjunto de sus consecuencias tautológicas puede no ser decidible (véase el capítulo III). Pero podemos obtener un resultado más débil que, en cierto sentido, es la mitad de la decidibilidad.

Llamemos a un conjunto A de expresiones *efectivamente numerable* sii existe algún procedimiento efectivo que produzca una lista, en algún orden, de los elementos de A. Si A es infinito, entonces tal vez el procedimiento nunca termine. Pero, a la larga (es decir, después de un tiempo finito), cualquier elemento particular de A debe aparecer en la lista.

Para que el lector pueda apreciar mejor esta noción, enunciaremos ahora una manera equivalente de formularla.

***Teorema 17E** Un conjunto A de expresiones es efectivamente numerable sii existe un procedimiento efectivo que, dada cualquier expresión ε, produce la respuesta "sí" en el caso de que $\varepsilon \in A$.

Si $\varepsilon \notin A$, el procedimiento podría producir la respuesta "no"; lo más probable es que continúe indefinidamente sin producir ninguna respuesta, pero no debe mentirnos y producir la respuesta "sí". Tal procedimiento se conoce como procedimiento de *semidecisión* (es la mitad de un procedimiento de decisión):

***Definición** Un conjunto A de expresiones es *semidecidible* sii existe un procedimiento efectivo tal que, dada una expresión ε, produce la respuesta "sí" sii $\varepsilon \in A$.

Así, el teorema 17E afirma que un conjunto es efectivamente numerable sii es semidecidible.

Demostración Si A es efectivamente numerable, entonces dada cualquier ε, podemos examinar la lista de los elementos de A mientras nuestro procedimiento la produce. Sólo cuando ε aparezca, decimos "sí". (Así, si $\varepsilon \notin A$, no se da ninguna respuesta. Esto es lo que impide que A sea decidible. Si ε no ha aparecido entre los primeros 10^{10} elementos enumerados de A, en general no hay manera de saber si $\varepsilon \notin A$ —en cuyo caso deberíamos dejar de buscarlo— o si ε aparecerá justamente en el siguiente paso.)

A la inversa, supongamos que tenemos el procedimiento descrito en el teorema y queremos crear una lista de los elementos de A. La idea es enumerar todas las expresiones y aplicar nuestro procedimiento dado a cada una, pero debemos administrar el tiempo de manera razonable. Es bastante fácil enumerar efectivamente todas las expresiones:

$$\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$$

Luego procedemos de acuerdo con el siguiente plan:

1. Dedicar un minuto a verificar si ε_1 es elemento de A (usando el procedimiento dado).

2. Dedicar dos minutos a verificar ε_1, luego dos minutos a ε_2.

3. Dedicar tres minutos a ε_1, luego tres minutos a ε_2, y tres minutos a ε_3.

Y así sucesivamente. Por supuesto, siempre que nuestro procedimiento produzca un "sí", colocaremos la expresión aceptada en la lista de salida. De esta manera llegará un momento en que todo elemento de A aparecerá en la lista. (Aparecerá una infinidad de veces a menos que modifiquemos las instrucciones anteriores para evitar la duplicación.) ⊣

Queda claro que cualquier conjunto decidible es también semidecidible. (Aun si el foco que indica "no" estuviera fundido, tendremos un procedimiento de semidecisión.) De aquí que todo conjunto decidible sea efectivamente numerable.

***Teorema 17F** Un conjunto de expresiones es decidible sii tanto él como su complemento (con respecto al conjunto de todas las expresiones) son efectivamente numerables.

Demostración Ejercicio 8. Algunas veces este resultado se conoce como "teorema de Kleene". ⊣

Obsérvese que si los conjuntos A y B son efectivamente numerables, entonces también lo son $A \cup B$ y $A \cap B$ (Ejercicio 11). La clase de los conjuntos decidibles también es cerrada bajo unión e intersección y además lo es bajo complementación.

Ahora un resultado más sustancial:

***Teorema 17G** Si Σ es un conjunto decidible de fórmulas, entonces el conjunto de las consecuencias tautológicas de Σ es efectivamente numerable.

Demostración De hecho, basta con que Σ esté efectivamente enumerado; consideremos una enumeración

$$\sigma_1, \sigma_2, \sigma_3, \ldots$$

Dada cualquier fórmula τ, podemos verificar sucesivamente (por medio de las tablas de verdad) si es que

$$\emptyset \models \tau,$$
$$\{\sigma_1\} \models \tau,$$
$$\{\sigma_1, \sigma_2\} \models \tau,$$
$$\{\sigma_1, \sigma_2, \sigma_3\} \models \tau,$$

etcétera. Si alguna de estas condiciones se cumple, entonces contestamos "sí". Si no, continuamos probando.

Esto produce una respuesta afirmativa siempre y cuando $\Sigma \models \tau$, por el corolario al teorema de compacidad. ⊣

Más adelante nos hará falta usar procedimientos efectivos para calcular funciones. Diremos que una función f es *efectivamente calculable* (o simplemente *calculable*) sii existe un procedimiento efectivo que, dada una entrada x, produzca a la larga la salida correcta $f(x)$.

Ejercicios

1. Supongamos que todo subconjunto finito de Σ es satisfactible. Pruebe que también lo es al menos uno de los conjuntos $\Sigma; \alpha$ y $\Sigma; \neg\alpha$. (Esto forma parte de la demostración del teorema de compacidad.) *Sugerencia*: Si no lo es, entonces $\Sigma_1; \alpha$ y $\Sigma_2; \neg\alpha$ son no satisfactibles para algunos subconjuntos finitos $\Sigma_1 \subseteq \Sigma$ y $\Sigma_2 \subseteq \Sigma$. Considere $\Sigma_1 \cup \Sigma_2$.

2. Sea Δ un conjunto de fórmulas tal que (i) todo subconjunto finito de Δ es satisfactible, y (ii) para toda fórmula α, o bien $\alpha \in \Delta$ o bien $(\neg\alpha) \in \Delta$. Definamos la asignación de verdad v:

$$v(A) = \begin{cases} V & \text{sii} \quad A \in \Delta, \\ F & \text{sii} \quad A \notin \Delta \end{cases}$$

para cada símbolo de enunciado A. Pruebe que para toda fórmula φ, $\bar{v}(\varphi) = V$ sii $\varphi \in \Delta$. (Esto forma parte de la demostración del teorema de compacidad.) *Sugerencia*: Use inducción sobre φ.

3. Pruebe que a partir del corolario del teorema de compacidad podemos demostrar el teorema de compacidad mismo (mucho más fácilmente que si no lo supusiéramos).

4. En 1977 se probó que todo mapa plano puede colorearse con cuatro colores. Desde luego, la definición de "mapa" requiere que haya sólo un número finito de países. Pero ampliando el concepto, supongamos que tenemos un mapa plano infinito (pero numerable) con los países C_1, C_2, $C_3, \ldots$ Demuestre que este mapa plano infinito también puede colorearse con cuatro colores. (*Sugerencia*: Divida los símbolos de enunciado en cuatro partes. Por ejemplo, un símbolo de enunciado puede usarse para traducir "El país C_7 se colorea de rojo". Forme un conjunto Σ_1 de fórmulas que digan, por ejemplo, C_7 es exactamente de uno de los colores. Forme otro conjunto Σ_2 de fórmulas que digan, para cada par de países fronterizos, que no son del mismo color. Aplique compacidad a $\Sigma_1 \cup \Sigma_2$.)

5. Dado un conjunto de fórmulas Σ, definimos una ***deducción*** a partir de Σ como una sucesión finita $\langle \alpha_0, \ldots, \alpha_n \rangle$ de fórmulas, tal que para cada $k \leq n$, o bien (a) α_k es una tautología, o (b) $\alpha_k \in \Sigma$, o (c) α_i es $(\alpha_j \rightarrow \alpha_k)$ para alguna i y alguna j menores que k. (En el caso (c) decimos que α_k se obtiene por *modus ponens* a partir de α_i y de α_j.) Haga una deducción a partir del conjunto

$$\{\neg \mathbf{S} \vee \mathbf{R}, \mathbf{R} \rightarrow \mathbf{P}, \mathbf{S}\}$$

cuyo último elemento es **P**.

6. Sea $\langle \alpha_0, \ldots, \alpha_n \rangle$ una deducción a partir de un conjunto de fórmulas Σ, como en el problema anterior. Pruebe que $\Sigma \models \alpha_k$ para cada $k \leq n$. *Sugerencia*: Use inducción fuerte sobre k, de modo que la hipótesis inductiva sea que $\Sigma \models \alpha_i$ para toda $i < k$.

7. Pruebe que si $\Sigma \models \tau$, entonces existe una deducción a partir de Σ, cuyo último elemento es τ. *Observación*: Este resultado se conoce como "completud"; los conceptos de los ejercicios 5-7 volverán a aparecer en la sección 4 del capítulo **II**.

8. Demuestre el teorema 17F. *Observación:* Dos procedimientos de semidecisión forman un todo.

*9. Las nociones de decidibilidad y enumerabilidad efectiva no sólo son aplicables a conjuntos de expresiones, sino también a conjuntos de enteros o a conjuntos de parejas de expresiones o de enteros. Pruebe que un conjunto A de expresiones es efectivamente numerable sii existe un conjunto decidible B de parejas $\langle\alpha, n\rangle$ (que constan de una expresión α y un entero n) tal que $A = \operatorname{dom} B$.

10. Sea Σ un conjunto efectivamente numerable de fórmulas. Suponga que para cada fórmula τ, o $\Sigma \models \tau$, o $\Sigma \models \neg\tau$. Pruebe que el conjunto de las consecuencias tautológicas de Σ es decidible.
    (a) Hágalo considerando que "o" se interpreta en el sentido exclusivo: o bien $\Sigma \models \tau$, o bien $\Sigma \models \neg\tau$, pero no ambos.
    (b) Hágalo considerando que "o" se interpreta en el sentido inclusivo: o $\Sigma \models \tau$, o $\Sigma \models \neg\tau$, o ambos.

11. (a) Explique por qué la unión de dos conjuntos efectivamente numerables también es efectivamente numerable.
    (b) Explique por qué la intersección de dos conjuntos efectivamente numerables también es efectivamente numerable.

12. Para cada una de las siguientes condiciones, dé un ejemplo de un conjunto de fórmulas *no satisfactible* Γ que cumple la condición.
    (a) Cada elemento de Γ es, en sí mismo, satisfactible.
    (b) Para cualesquiera *dos* elementos γ_1 y γ_2 de Γ, el conjunto $\{\gamma_1, \gamma_2\}$ es satisfactible.
    (c) Para cualesquiera *tres* elementos γ_1, γ_2 y γ_3 de Γ, el conjunto $\{\gamma_1, \gamma_2, \gamma_3\}$ es satisfactible.

II

LÓGICA DE PRIMER ORDEN

0. *Comentarios preliminares*

En el capítulo anterior se presentó el primero de nuestros modelos matemáticos de pensamiento deductivo. Ese modelo es muy simple, de hecho, *demasiado* simple. Es fácil pensar en ejemplos de deducciones intuitivamente correctas que no pueden ser reflejadas adecuadamente en un modelo de lógica de enunciados.

Supongamos que comenzamos con una serie de hipótesis (en español) y una posible conclusión. Al traducir todo esto al lenguaje de la lógica de enunciados, tendremos un conjunto Σ de hipótesis y una posible conclusión τ. Ahora bien, si tenemos que $\Sigma \models \tau$, sentimos entonces que la deducción original en español era válida; pero si encontramos que $\Sigma \not\models \tau$, entonces no tendremos certeza. Es posible que esto se deba a que el modelo de la lógica de enunciados es demasiado tosco para reflejar la sutileza de la deducción original.

Este capítulo presenta un sistema lógico con mucha mayor capacidad. De hecho, cuando el "matemático activo" encuentra una prueba, casi invariablemente dicha prueba se podrá reflejar en el sistema presentado en este capítulo.

En primer lugar, queremos hacer una descripción informal de las características que podrían tener nuestros lenguajes de primer orden (o al menos de las que son capaces de simular). Comenzamos con un caso especial, el lenguaje de primer orden para la teoría de los números. Para este lenguaje existe una manera a propósito de traducirlo al español y de éste a aquél (Tabla VII).

Tabla VII

Expresión formal	Traducción
$\mathbf{0}$	"Cero." Aquí, $\mathbf{0}$ es un símbolo de constante que representará al número 0.
$\mathbf{S}t$	"El sucesor de t." Aquí, $\mathbf{S}$ es un símbolo de función de un argumento. t se considerará como una expresión para representar algún número a. Entonces, $\mathbf{S}t$ nombra a $S(a)$, el sucesor de a. Por ejemplo, tenemos que $\mathbf{S0}$ representa al número 1.
$< v_1 v_2$	"v_1 es menor que v_2." Aquí, $<$ es un símbolo de predicado de dos argumentos. Al final de la sección 1 del capítulo II adoptaremos convenciones que nos permitirán abreviar la expresión en un estilo más común: $v_1 < v_2$.
$\forall$	"Para todo número natural." El símbolo $\forall$ es el símbolo de cuantificador universal. De una forma más general, con cada traducción del lenguaje al español habrá determinado conjunto asociado A (usualmente llamado el universo); $\forall$ será entonces "para todo elemento del universo A".
$\forall v_1 < \mathbf{0} v_1$	"Para todo número natural v_1, cero es menor que v_1." O de una manera más eufónica: "Todo número natural es mayor que 0." Este enunciado formal es falso con el significado de la traducción, ya que cero no es mayor que sí mismo.

Se menciona una abreviatura en la Tabla VII y habrá otras más (Tabla VIII, de la p. 105).

En realidad no seremos tan generosos como las tablas lo sugieren. Hay dos medidas de carácter económico que podemos poner en práctica para simplificar sin ninguna pérdida esencial de expresividad lingüística:

En primer lugar, elegiremos como nuestros símbolos de conectivo para enunciados solamente $\neg$ y $\rightarrow$. Como se mencionó anteriormente en la sección 5 del capítulo I, sabemos que éstos

Tabla VIII

Expresión abreviada	Traducción
$x = y$	"x es igual a y". En la forma no abreviada, esto se convertiría en $= xy$.
$\exists v$	"Existe un número natural v tal que", o de una manera más general, "existe un elemento del universo tal que".
$\exists v_1 \, \forall v_2 \, v_1 = v_2$	"Existe exactamente un número natural." De nuevo, este enunciado formal resulta falso con el significado de la traducción.
$\forall v_1 (0 < v_1 \vee 0 = v_1)$	"Todo número natural es mayor o igual que cero."

forman un conjunto completo y por lo mismo no hay una razón que obligue a utilizar más.

En segundo lugar, renunciamos al lujo de tener un cuantificador existencial, $\exists x$. En lugar de éste usamos $\neg \forall x \neg$. Esto se justifica, ya que una oración en español tal como

Hay algo podrido en Dinamarca

es equivalente a

No es el caso que para todo x, x no está podrido en Dinamarca.

Por lo tanto, la fórmula $\exists v_1 \, \forall v_2 \, v_1 = v_2$ se convierte, en forma no abreviada, en

$$(\neg \forall v_1 (\neg \forall v_2 = v_1 \, v_2)).$$

Como ejemplo de un lenguaje a propósito para el caso, podríamos traducir "Sócrates es un hombre" como Hs, donde H es un símbolo de predicado de un argumento que se utiliza para traducir "es un hombre" y s es un símbolo de cons-

tante que se utiliza para nombrar a Sócrates. De manera similar, para traducir "Sócrates es mortal", utilizamos Ms. Por lo tanto, "Todos los hombres son mortales" se traduce como $\forall v_1(Hv_1 \to Mv_1)$.

Es posible que el lector reconozca los símbolos $\forall$ y $\exists$ a partir de contextos matemáticos anteriores. De hecho, cuando en sus exposiciones escriben en el pizarrón, algunos matemáticos ya utilizan un lenguaje casi totalmente formalizado, con sólo unos cuantos vestigios del español. El hecho de que nuestros lenguajes de primer orden se asemejen al de ellos no es un mero accidente. Queremos que sea posible dar un paso atrás y estudiar no sólo los conjuntos o los grupos, sino además los enunciados de la teoría de grupos o de conjuntos. (Algunas veces se usa el término *metamatemáticas*; dicha palabra sugiere el procedimiento de dar un paso atrás para examinar lo que el matemático está haciendo.) Los objetos que ahora estudia usted, el lógico, son los enunciados que usted, el teórico, utilizó anteriormente en el estudio de los conjuntos. Esto requiere formalizar el lenguaje de la teoría de conjuntos, y nosotros deseamos incorporar a nuestros lenguajes formales las características utilizadas, por ejemplo, en la teoría de conjuntos.

1. *Lenguajes de primer orden*

En lo sucesivo asumiremos que tenemos un número infinito de objetos distintos (que denominamos símbolos), ordenados de acuerdo con lo siguiente:

A. Símbolos lógicos

0. Paréntesis: (,).
1. Símbolos de conectivo para enunciados: $\to$, $\neg$.
2. Variables (una para cada entero positivo n):

$$v_1, v_2, \ldots$$

3. Símbolo de igualdad (opcional): $=$.

B. Parámetros

0. Símbolo de cuantificador: $\forall$.

1. Símbolos de predicado: para cada entero positivo n, algún conjunto (posiblemente vacío) de símbolos, denominado símbolos de predicado de n argumentos.
2. Símbolos de constante: algún conjunto (posiblemente vacío) de símbolos.
3. Símbolos de función: para cada entero positivo n, algún conjunto (posiblemente vacío) de símbolos, denominados símbolos de función de n argumentos.

En A.3 permitimos la posibilidad de existencia del símbolo de igualdad, pero no damos por hecho su presencia. Algunos lenguajes contarán con él y otros no. El símbolo de igualdad es un símbolo de predicado de dos argumentos, pero se distingue de otros símbolos de predicados de dos argumentos por ser un símbolo lógico más que un parámetro. (Este estado afectará su comportamiento cuando se traduzca al español.) Es necesario que asumamos que se encuentra presente algún símbolo de predicado de n argumentos para algún n.

En B.2, los símbolos de constante también se llaman símbolos de función de 0 argumentos. Con frecuencia, esto permitirá dar un tratamiento uniforme a los símbolos que se encuentran en B.2 y B.3.

Al igual que antes, asumimos que cada símbolo es distinto y ningún símbolo es una sucesión finita de otros símbolos.

Con el fin de especificar qué lenguaje tenemos ante nosotros (que difiere de otros lenguajes de primer orden), debemos: (i) decir si se encuentra presente o no el símbolo de igualdad, y (ii) decir cuáles son los parámetros.

A continuación damos una lista de algunos ejemplos de lo que sería este lenguaje:

1. *Lenguaje puro de predicados*

Igualdad: no.
Símbolos de predicado de n argumentos: $A_1^n, A_2^n, \ldots$
Símbolos de constante: $a_1, a_2, \ldots$
Símbolos de función de n argumentos ($n > 0$): ninguno.

2. *Lenguaje de la teoría de conjuntos*

Igualdad: sí (normalmente).

Parámetros de predicado: un símbolo de predicado de dos argumentos $\in$.

Símbolos de función: ninguno (u ocasionalmente un símbolo de constante $\emptyset$).

3. *Lenguaje de la teoría elemental de números* (como en el capítulo III)

Igualdad: sí.

Parámetros de predicado: un símbolo de predicado de dos argumentos $<$.

Símbolos de constante: el símbolo $\mathbf{0}$.

Símbolos de función de un argumento: S (para el sucesor).

Símbolos de función de dos argumentos: $+$ (para la suma), $\cdot$ (para la multiplicación), y $\mathbf{E}$ (para la exponenciación).

En los ejemplos 2 y 3 hay ciertas traducciones usuales para los parámetros. A continuación presentamos varios ejemplos de enunciados que pueden traducirse a estos lenguajes y unos cuantos ejemplos de enunciados que no pueden ser traducidos así.

Es importante notar que nuestra noción de lenguaje incluye el lenguaje de la teoría de conjuntos. Se suele aceptar que, en general, las matemáticas se pueden representar en la teoría de conjuntos. Esto significa que:

(a) Los enunciados en matemáticas (como el teorema fundamental del cálculo) pueden expresarse en el lenguaje de la teoría de conjuntos; y

(b) Los teoremas de matemáticas son consecuencia lógica de los axiomas de la teoría de conjuntos.

Nuestro modelo de lógica de primer orden es totalmente adecuado para reflejar este procedimiento.

Ejemplos en el lenguaje de la teoría de conjuntos. Aquí se pretende que $\forall$ signifique "para todos los conjuntos" y $\in$ signifique "es elemento de".

1. "No existe un conjunto del cual todo conjunto sea elemento." Traduciremos esto al lenguaje de la teoría de conjuntos en varios pasos. Los enunciados intermedios

no están ni en español ni en lenguaje formal, sino en una mezcla de ambos.

$\neg$ [Existe un conjunto del cual todo conjunto es elemento]

$\neg \exists v_1$ [Todo conjunto es elemento de v_1]

$\neg \exists v_1 \forall v_2 \quad v_2 \in v_1$

Aunque resulta tentador detenernos aquí, ahora debemos reemplazar $v_2 \in v_1$ por $\in v_2 v_1$, debido a que los símbolos de predicado siempre irán a la izquierda en dichos contextos. Además se deberá reemplazar $\exists v_1$ y poner en su lugar $\neg \forall v_1 \neg$, tal como se mencionó anteriormente. Debemos utilizar el número correcto de paréntesis. El producto terminado es:

$$(\neg (\neg \forall v_1 (\neg \forall v_2 \in v_2 v_1))).$$

2. Axioma del par: "Para cualesquiera dos conjuntos, existe un conjunto cuyos elementos son exactamente los dos conjuntos dados." De nuevo traduciremos por pasos.

$\forall v_1 \ \forall v_2$ [Existe un conjunto cuyos elementos son precisamente v_1 y v_2]

$\forall v_1 \ \forall v_2 \ \exists v_3$ [Los elementos de v_3 son exactamente v_1 y v_2]

$\forall v_1 \ \forall v_2 \ \exists v_3 \ \forall v_4 \ (v_4 \in v_3 \leftrightarrow v_4 = v_1 \lor v_4 = v_2)$

Ahora reemplazaremos $\exists v_3$ por $\neg \forall v_3 \neg$, $v_4 \in v_3$ por $\in v_4 v_3$ y $v_4 = v_i$ por $= v_4 v_i$. Además, debemos eliminar $\leftrightarrow$ y $\lor$ en favor de los conectivos elegidos $\rightarrow$ y $\neg$. Entonces,

$$\alpha \lor \beta \text{ se convierte en } \neg \alpha \rightarrow \beta;$$
$$\alpha \leftrightarrow \beta \text{ se convierte en } \neg ((\alpha \rightarrow \beta) \rightarrow \neg (\beta \rightarrow \alpha)).$$

El producto terminado es

$$\forall v_1 \ \forall v_2 (\neg \forall v_3 (\neg \forall v_4 (\neg ((\in v_4 v_3 \rightarrow ((\neg = v_4 v_1) \rightarrow$$
$$= v_4 v_2)) \rightarrow (\neg (((\neg = v_4 v_1) \rightarrow = v_4 v_2) \rightarrow \in v_4 v_3)))))).$$

El producto terminado no resulta ni por asomo tan fácil de leer como la versión que le precedió. Ya que no tenemos interés en hacernos deliberadamente la vida difícil, a la larga adoptaremos reglas convencionales que nos permitan evitar ver el producto terminado. Pero por el momento se considerará lo anterior como una novedad interesante aunque poco atractiva.

Ejemplos en el lenguaje de la teoría elemental de los números. Aquí se pretende que $\forall$ signifique "para todos los números naturales" y que $<$, $\mathbf{0}$, $+$, $\cdot$ y $\mathbf{E}$ tengan sus significados obvios.

1. Como nombre para el número natural 2 tenemos el término **SS0**, ya que 2 es el sucesor del sucesor del cero. De forma similar, para el 4 tenemos el término **SSSS0**. Para la frase "2 + 2" resulta tentador utilizar **SS0** + **SS0**; pero adoptaremos la convención de poner siempre a la izquierda el símbolo de función (es decir, utilizaremos la notación polaca para los símbolos de funciones); entonces tendremos que para la frase en español "2 + 2" usaremos el término + **SS0 SS0**. El enunciado en español "dos más dos es cuatro" se traduce como

$$= + \mathbf{SS0}\,\mathbf{SS0}\,\mathbf{SSSS0}$$

(Los espacios se insertaron para ayudar al lector, pero no constituyen una característica oficial del lenguaje.)

2. "Cualquier número natural distinto de cero es el sucesor de algún número." Realizaremos la traducción en tres pasos:

$\forall v_1$ [Si v_1 es diferente de cero, entonces v_1 es el sucesor de algún número.]

$\forall v_1 (v_1 \neq \mathbf{0} \rightarrow \exists v_2\, v_1 = \mathbf{S}\, v_2)$.

$\forall v_1 ((\neg = v_1 \mathbf{0}) \rightarrow (\neg \forall v_2 (\neg = v_1 \mathbf{S} v_2)))$.

3. "Cualquier conjunto no vacío de números naturales tiene un elemento mínimo." Esto no puede traducirse a nuestro lenguaje, porque no podemos expresar "cualquier . . . conjunto". Esto requiere algo como el lenguaje

(de primer orden) para la teoría de conjuntos o un lenguaje de segundo orden para la teoría de los números. De cualquier manera, podríamos traducir "El conjunto de primos tiene un elemento mínimo." (El primer paso es convertir este enunciado en "hay un mínimo primo". Dejamos los pasos restantes al lector; algunas sugerencias para resolverlo se encuentran en la siguiente sección.)

EJEMPLOS en lenguajes *ad hoc*.

1. "Todas las manzanas están malas."

$$\forall v_1 \, (A\, v_1 \rightarrow B\, v_1).$$

2. "Algunas manzanas están malas."
Paso intermedio: $\exists v_1 \, (A\, v_1 \wedge B v_1)$.
Producto terminado: $(\neg \forall v_1 \, (\neg \, (\neg \, (A v_1 \rightarrow (\neg B v_1)))))$.

Estos dos ejemplos ilustran patrones que surgen continuamente. Un enunciado en español que afirma que, en una determinada categoría, todo tiene alguna propiedad se traduce como:

$$\forall v \, (__ \rightarrow __).$$

Un enunciado que afirma que en la categoría hay algún objeto o algunos objetos que tienen la propiedad se traduce como:

$$\exists\, v \, (__ \wedge __).$$

El lector deberá tener precaución para no confundir estos dos patrones; por ejemplo,

$$\forall v_1 (A v_1 \wedge B v_1)$$

se traduce como "Toda cosa es una manzana y está mala", que es un enunciado mucho más fuerte que el del primer ejemplo. De forma similar, $\exists\, v_1 \, (A\, v_1 \rightarrow B\, v_1)$ traduce "Existe algo que está malo, si es una manzana".

Esta afirmación es mucho más débil que el enunciado del segundo ejemplo. Es verdadero (por vacuidad), aun si todas las manzanas están buenas, considerando solamente que el mundo tenga alguna otra cosa que no sea una manzana.

3. "El papá de Roberto puede ganarle al papá de cualquier otro niño de la cuadra." Establezca un lenguaje en donde $\forall$ signifique "para toda la gente", Kx signifique "x es un niño de la cuadra", b signifique "Roberto", Bxy traduzca "x puede ganarle a y", y fx signifique "el papá de x". Entonces una traducción es:

$$\forall v_1(Kv_1 \to ((\neg = v_1 b) \to B f b f v_1)).$$

4. En cálculo aprendemos el significado de "la función f converge a L cuando x se aproxima a a":

$$\forall \varepsilon (\varepsilon > 0 \to \exists \delta (\delta > 0 \wedge \forall x (|x - a| < \delta \to |fx - L| < \varepsilon))).$$

Esto es, aparte de los asuntos de notación, una fórmula del tipo que nos interesa, que utiliza un símbolo de predicado para el orden, símbolos de función para f, resta y valores absolutos, y símbolos de constante para 0, a y L.

Fórmulas

Una *expresión* es una sucesión finita de símbolos. Por supuesto, la mayoría de las expresiones son absurdas, pero existen ciertas expresiones interesantes: los términos y las fórmulas.

Los términos son los sustantivos y los pronombres de nuestro lenguaje; pueden entenderse como las expresiones que nombran a los objetos. Las fórmulas atómicas serán aquellas fórmulas que no tengan ni símbolos de conectivo ni símbolos de cuantificador.

Términos	Fórmulas atómicas	Otras fórmulas	Todas las demás expresiones

Fórmulas (abarca: Fórmulas atómicas, Otras fórmulas)

Los términos se definen como aquellas expresiones que pueden construirse a partir de los símbolos de constante y de las variables al prefijarles los símbolos de función. Para volver a enunciar esto en la terminología del capítulo I, definimos para cada símbolo de función f de n argumentos, una operación de construcción de términos $\mathcal{F}_f$ de n argumentos sobre las expresiones:

$$\mathcal{F}_f(\varepsilon_1, \ldots, \varepsilon_n) = f\varepsilon_1 \cdots \varepsilon_n.$$

Definición El conjunto de *términos* es el conjunto de expresiones que pueden construirse a partir de símbolos de constante y variables al aplicar (cero o más veces) las operaciones $\mathcal{F}_f$.

Si no hay símbolos de función (además de los símbolos de constante), entonces los términos serán únicamente los símbolos de constante y las variables. Para este caso no necesitamos una definición inductiva.

Nótese que utilizamos notación polaca para los términos, al ubicar el símbolo de función a la izquierda. Los términos no contienen paréntesis ni comas. Más adelante probaremos un resultado de unicidad de la lectura, mostrando que dado un término, podemos descomponerlo sin ambigüedades.

Los términos son las expresiones que se traducen como los nombres de los objetos (o frases nominales), en contraste con las fórmulas, que se traducen como afirmaciones acerca de los objetos.

Algunos ejemplos de términos en el lenguaje de la teoría de los números son

$$+ \, v_2 \, \mathbf{S0},$$
$$\mathbf{SSSS0},$$
$$+ \, \mathbf{E} v_1 \, \mathbf{SS0} \, \mathbf{E} v_2 \, \mathbf{SS0}.$$

Las fórmulas atómicas desempeñarán un papel más o menos análogo al que desempeñan los símbolos de enunciado en la lógica de enunciados. Una *fórmula atómica* es una expresión de la forma

$$Pt_1 \cdots t_n,$$

donde P es un símbolo de predicado de n argumentos y $t_1, \cdots, t_n$ son términos.

Por ejemplo, $= v_1 v_2$ es una fórmula atómica, ya que $=$ es un símbolo de predicado de dos argumentos y cada variable es un término. En el lenguaje de la teoría de conjuntos tenemos la fórmula atómica $\in v_5 v_3$.

Nótese que las fórmulas atómicas no se definen de forma inductiva. En lugar de hacerlo, nos hemos limitado a decir explícitamente cuáles expresiones son fórmulas atómicas.

Las *fórmulas* (o *fórmulas bien formadas*) son aquellas expresiones que pueden construirse a partir de las fórmulas atómicas mediante el uso (cero o más veces) de los símbolos de conectivo y del símbolo de cuantificador. Podemos volver a expresar esto usando la terminología del capítulo I si definimos primero algunas operaciones de construcción de fórmulas sobre las expresiones:

$$\mathcal{E}_{\neg}(\gamma) = (\neg\gamma),$$
$$\mathcal{E}_{\rightarrow}(\gamma, \delta) = (\gamma \rightarrow \delta),$$
$$\mathcal{Q}_i(\gamma) = \forall v_i\, \gamma.$$

Definición El conjunto de las *fórmulas* es el conjunto de expresiones que pueden construirse a partir de las fórmulas atómicas al aplicar (cero o más veces) las operaciones $\mathcal{E}_{\neg}$, $\mathcal{E}_{\rightarrow}$ y $\mathcal{Q}_i (i = 1, 2, \ldots)$.

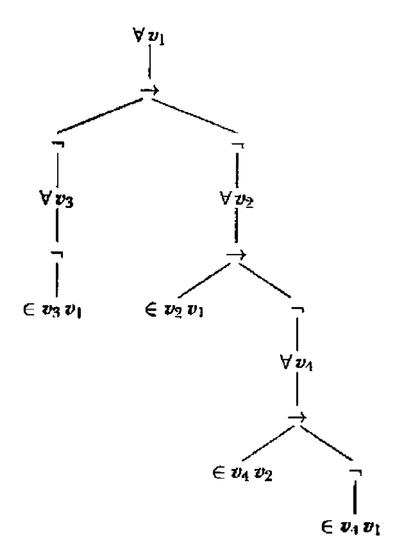
Por ejemplo, por una parte tenemos que $\neg v_3$ no es una fórmula. (¿Por qué?) Por otra parte,

$$\forall v_1 ((\neg \forall v_3 (\neg \in v_3 v_1)) \rightarrow (\neg \forall v_2 (\in v_2 v_1 \rightarrow (\neg \forall v_4 (\in v_4 v_2 \rightarrow (\neg \in v_4 v_1))))))$$

es una fórmula, como lo demuestra el árbol de la página siguiente. Pero se requiere cierta cantidad de estudio para descubrir que esta fórmula es el axioma de regularidad de la teoría de conjuntos.

Variables libres

Dos ejemplos de fórmulas son $\forall v_2 \in v_2 v_1$ y $(\neg \forall v_1 (\neg \forall v_2 \in v_2 v_1))$. No obstante, hay una importante diferencia entre estos dos ejemplos. El segundo podría traducirse como:



Existe un conjunto tal que todo conjunto es elemento suyo.

Sin embargo, el primer ejemplo sólo puede traducirse como un enunciado incompleto:

Todo conjunto es elemento de $_____1$.

No nos es posible terminar el enunciado sin saber qué hacer con v_1. En este tipo de casos, diremos que v_1 *ocurre libre* en la fórmula $\forall v_2 \in v_2 v_1$. En contraste, no hay variables que ocurran libremente en $(\neg\forall v_1(\neg\forall v_2 \in v_2 v_1))$. Pero, por supuesto, necesitamos una definición precisa que no requiera referirse a las posibles traducciones al español, sino que se remita únicamente a los símbolos mismos.

Consideremos cualquier variable x. Definimos para cada fórmula α, lo que significa que x *ocurre libre* en α. Hacemos esto por recursión:

1. Para α atómica, x ocurre libre en α sii x ocurre en (es decir, es símbolo de) α.

2. x ocurre libre en $(\neg\alpha)$ sii x ocurre libre en α.

3. x ocurre libre en $(\alpha \rightarrow \beta)$ sii x ocurre libre en α o en β.

4. x ocurre libre en $\forall v_i \alpha$ sii x ocurre libre en α y $x \neq v_i$.

Esta definición usa implícitamente el teorema de recursión. Podemos reformular la situación en términos de funciones. Comenzamos con la función h, que se define en fórmulas atómicas:

$h(\alpha) =$ el conjunto de todas la variables, si existe alguna, en la fórmula atómica α.

Y queremos extender h a una función $\bar{h}$ definida en todas las fórmulas de tal manera que

$$\bar{h}(\mathcal{E}_{\neg}(\alpha)) = \bar{h}(\alpha),$$
$$\bar{h}(\mathcal{E}_{\rightarrow}(\alpha,\beta)) = \bar{h}(\alpha) \cup \bar{h}(\beta),$$
$$\bar{h}(\mathcal{Q}_i(\alpha)) = \bar{h}(\alpha) \text{ después de quitar } v_i \text{ si se encuentra presente.}$$

Entonces podemos decir que x ocurre libre en α (o que x es una *variable libre* de α). La existencia de una única $\bar{h}$ (y he aquí lo significativo de nuestra definición) se sigue del teorema de recursión de la sección 4 del capítulo I y del hecho (comprobado en la sección 3 de este capítulo) de que cada fórmula tiene una descomposición única.

Si ninguna variable ocurre libre en la fórmula α (es decir, si $\bar{h}(\alpha) = \emptyset$), entonces α es un enunciado. (Los enunciados son, de manera intuitiva, las fórmulas que pueden traducirse sin espacios en blanco al español, una vez que se nos ha dicho cómo interpretar los parámetros.)

Por ejemplo, $\forall v_2(Av_2 \rightarrow Bv_2)$ y $\forall v_3(Pv_3 \rightarrow \forall v_3 Qv_3)$ son enunciados; pero v_1 ocurre libre en $(\forall v_1 Av_1 \rightarrow Bv_1)$. Normalmente, los enunciados son las fórmulas más interesantes. Las demás fórmulas tienen una existencia de segunda clase, y se usan principalmente como bloques de construcción de los enunciados.

Al traducir un enunciado del español, resulta irrelevante la elección de variables particulares. Anteriormente tradujimos

"todas las manzanas están malas" como $\forall v_1(A v_1 \rightarrow B v_1)$; pero de igual manera podríamos haber utilizado

$$\forall v_{27}(A v_{27} \rightarrow B v_{27}).$$

De hecho, la variable se utiliza como un pronombre, tal como podríamos decir en español "para cualquier objeto dado, si *él* es una manzana, entonces *él* está malo". (Hemos incorporado a nuestro lenguaje una cantidad adecuada de pronombres: $él_1$, $él_2, \ldots$) Ya que la elección de variables particulares carece de importancia, frecuentemente ni siquiera especificaremos la elección. En lugar de hacerlo, escribiremos, por ejemplo, $\forall x(A x \rightarrow B x)$, donde se entiende que x es alguna variable. (Lo intrascendente de la elección de la variable se convertirá finalmente en un teorema.)

En otras áreas de las matemáticas, las variables se usan de manera similar. Así, tenemos que en

$$\sum_{i=1}^{7} a_{ij}$$

i es una variable "simulada", pero j ocurre libre.

Acerca de la notación

Podemos especificar una fórmula (o de hecho, cualquier expresión) al escribir una línea que muestre explícitamente cada símbolo. Por ejemplo,

$$\forall v_1((\neg = v_1\, 0) \rightarrow (\neg \forall v_2(\neg = v_1\, \mathbf{S} v_2))).$$

Pero esta manera de escribir las cosas, aunque es generosa en su completud, puede no resultar inmediatamente comprensible. La incomprensibilidad se debe (en parte) a las simplificaciones que queremos para nuestro lenguaje (tales como la falta de un símbolo de cuantificador existencial). Es natural que queramos tener nuestro premio y disfrutar de él, así que ahora acordaremos los métodos para especificar las fórmulas de maneras más indirectas pero más legibles. Estas convenciones nos permitirán escribir una expresión como

$$\forall v_1(v_1 \neq 0 \to \exists v_2\, v_1 = Sv_2)$$

para nombrar la misma fórmula escrita anteriormente.

Nótese bien que *no* estamos cambiando nuestra definición de lo que es una fórmula. Únicamente estamos urdiendo la manera de fijar ciertas formas de nombrar fórmulas. En los casos (raros) en que la sucesión exacta de símbolos resulta importante, es posible que tengamos que hacer a un lado estas nuevas convenciones y volver a utilizar la notación primitiva.

Entonces adoptaremos las siguientes formas abreviadas y convenciones. Aquí, α y β son fórmulas, x es una variable y u y t son términos.

$(\alpha \vee \beta)$ es la abreviación de $((\neg\,\alpha) \to \beta)$.
$(\alpha \wedge \beta)$ es la abreviación de $(\neg\,(\alpha \to (\neg\,\beta)))$.
$(\alpha \leftrightarrow \beta)$ es la abreviación de $((\alpha \to \beta) \wedge (\beta \to \alpha))$; es decir,

$$(\neg\,((\alpha \to \beta) \to (\neg\,(\beta \to \alpha)))).$$

$\exists x\, \alpha$ es la abreviación de $(\neg \forall x(\neg\,\alpha))$.

$u = t$ es la abreviación de $= ut$. Una forma abreviada similar se aplica a algunos otros símbolos de funciones y de predicados de dos argumentos. Por ejemplo, $2 < 3$ abrevia $< 2\ 3$, y $2 + 2$ abrevia $+\ 2\ 2$.

$u \neq t$ abrevia $(\neg\ = ut)$; de forma similar, $u \not< t$ abrevia $(\neg < ut)$.

En cuanto a los paréntesis, no sólo utilizaremos (y), sino además [y], etc., y omitiremos la mención de tantos como nos resulte posible. Con ese fin, adoptaremos las siguientes convenciones:

1. Los paréntesis externos se pueden omitir. Por ejemplo, $\forall x\, \alpha \to \beta$ es $(\forall x\, \alpha \to \beta)$.

2. $\neg$, $\forall$ y $\exists$ se aplicarán a lo menos posible. Por ejemplo:

$$\neg\,\alpha \wedge \beta \text{ es } ((\neg\,\alpha) \wedge \beta), \text{ y no } \neg\,(\alpha \wedge \beta);$$
$$\forall x\, \alpha \to \beta \text{ es } (\forall x\, \alpha \to \beta), \text{ y no } \forall x\, (\alpha \to \beta);$$
$$\exists x\, \alpha \wedge \beta \text{ es } (\exists x\, \alpha \wedge \beta), \text{ y no } \exists x\, (\alpha \wedge \beta).$$

En dichos casos, incluso podemos agregar paréntesis gratuitos, como en $(\exists x\, \alpha) \wedge \beta$.

3. $\wedge$ y $\vee$ se aplicarán a lo menos posible, según lo establecido en la convención 2. Por ejemplo,

$$\neg\alpha \wedge \beta \rightarrow \gamma \text{ es } ((\neg\alpha) \wedge \beta) \rightarrow \gamma.$$

4. Cuando se use repetidamente un conectivo, la expresión se agrupará a la derecha. Por ejemplo,

$$\alpha \rightarrow \beta \rightarrow \gamma \text{ es } \alpha \rightarrow (\beta \rightarrow \gamma).$$

Ejemplos de la manera en que podremos eliminar abreviaciones, reescribiendo la fórmula de una manera no abreviada que liste explícitamente cada símbolo en orden:

1. $\exists x (Ax \wedge Bx)$ es $(\neg\forall x (\neg(\neg(Ax \rightarrow (\neg Bx)))))$.
Pero $(\neg\forall x (Ax \rightarrow (\neg Bx)))$ sería una fórmula equivalente (en cualquier noción de equivalencia razonable).

2. $\exists x\, Ax \rightarrow Bx$ es $((\neg\forall x (\neg Ax)) \rightarrow Bx)$.
$\exists x (Ax \rightarrow Bx)$ es $(\neg\forall x (\neg(Ax \rightarrow Bx)))$.

Intentaremos utilizar los diversos alfabetos de una forma sistemática. La lista del sistema aparece en seguida, pero habrá excepciones ocasionales por razones especiales.

Símbolos de predicado: letras cursivas mayúsculas; también $\in$, $<$.

Variables: $\mathbf{v}_i$, u, v, x, y, z.

Símbolos de función: f, g, h; también $\mathbf{S}$, $+$, etcétera.

Símbolos de constante: $a, b, \ldots$; también $\mathbf{0}$.

Términos: u, t.

Fórmulas: letras griegas minúsculas.

Enunciados: σ, τ.

Conjuntos de fórmulas: letras griegas mayúsculas, además de ciertas letras cursivas que pretenden ser griegas, es decir, A (alfa) y T (tau).

Estructuras (véase la sección siguiente): letras alemanas mayúsculas (Fraktur).

Ejercicios

1. Suponga usted que tenemos un lenguaje con los parámetros siguientes: $\forall$ significa "para todas las cosas"; N significa "es un número"; I significa "es interesante"; $<$ significa "es menor que"; y $\mathbf{0}$ es un símbolo de constante que significa cero. Traduzca a este lenguaje los enunciados del español que aparecen abajo. Si el enunciado en español es ambiguo, necesitará más de una traducción.

   (a) Cero es menor que cualquier número.

   (b) Si cualquier número es interesante, entonces el cero es interesante.

   (c) Ningún número es menor que cero.

   (d) Cualquier número no interesante con la propiedad de que todos los números menores son interesantes es, desde luego, interesante.

   (e) No existe un número tal que todos los números sean menores que él.

   (f) No existe un número tal que ningún número sea menor que él.

2. Utilizando el mismo lenguaje del ejercicio anterior, traduzca a un buen español la fórmula

$$\forall x(Nx \rightarrow Ix \rightarrow \neg \forall y(Ny \rightarrow Iy \rightarrow \neg x < y)).$$

En los ejercicios 3 a 8, traduzca cada enunciado en español al lenguaje de primer orden especificado. (Puede realizar la traducción por pasos, al igual que en algunos de los ejemplos.) Haga uso pleno de las convenciones de notación y de las formas abreviadas, para hacer que el resultado final sea lo más legible que se pueda.

3. Ni a ni b son elementos de todo conjunto. ($\forall$, para todos los conjuntos; $\in$, es un elemento de; a, a; b, b.)

4. Si los caballos son animales, entonces las cabezas de caballos son cabezas de animales. ($\forall$, para todas las cosas; E, es un caballo; A, es un animal; hx, la cabeza de x.)

5. (a) A algunas personas se las puede engañar todo el tiempo. (b) Se puede engañar a todas las personas parte del tiempo. (c) No se puede engañar a todas las personas todo el tiempo. (∀, para todas las cosas; *P*, es una persona; *T*, es un tiempo; *Fxy*, se puede engañar a *x* en *y*. Uno o más de los enunciados anteriores puede ser ambiguo, en ese caso se necesitará más de una traducción.)

6. (a) Álvarez no puede realizar bien todos los trabajos. (b) Álvarez no puede realizar bien ningún trabajo. (∀, para todas las cosas; *J*, es un trabajo; *a*, Álvarez; *Dxy*, *x* puede realizar bien *y*.)

7. (a) A ninguna persona le caen bien todas las personas. (b) A ningún demócrata le cae bien todo republicano. (∀, para todas las personas; *Lxy*, a *x* le cae bien *y*; *D*, es un demócrata; *R*, es un republicano.)

8. (a) Todo granjero que tiene un burro necesita heno. (b) Todo granjero que tiene un burro lo golpea. (∀, para todas las cosas; *F*, es un granjero; *D*, es un burro; *Oxy*, *x* tiene a *y*; *H*, necesita heno; *Bxy*, *x* golpea a *y*.)

9. Dé una definición precisa de lo que significa para la variable *x* ocurrir libre como símbolo i-ésimo en la fórmula α. (Si *x* es el símbolo i-ésimo de α pero no ocurre libre ahí, entonces se dice que ocurre ahí de forma *acotada*.)

10. Reescriba cada una de las fórmulas siguientes de modo tal que aparezcan explícitamente y en su orden todos sus símbolos:

    (a) $\exists v_1 P v_1 \wedge P v_1$.

    (b) $\forall v_1 A v_1 \wedge B v_1 \rightarrow \exists v_2 \neg C v_2 \vee D v_2$.

    En cada caso, diga qué variables ocurren libres en la fórmula.

2. *Verdad y modelos*

En la lógica de enunciados tuvimos asignaciones de verdad que nos decían cuáles símbolos de enunciado se deberían de interpretar como verdaderos y cuáles como falsos. En la lógica de

primer orden, las *estructuras* desempeñan un papel análogo. Se puede pensar que las estructuras suministran el diccionario para traducir del lenguaje formal al español. (A veces, las estructuras se denominan *interpretaciones*, pero preferimos reservar esa palabra para otro concepto, que encontraremos en la sección 7 de este mismo capítulo.)

Una estructura para un lenguaje de primer orden nos dirá:

1. A qué colección de objetos se refiere el símbolo de cuantificador universal ($\forall$), y
2. Qué denotan los otros parámetros (los símbolos de función y de predicado).

Formalmente, una *estructura* $\mathfrak{A}$ para nuestro lenguaje dado de primer orden es una función cuyo dominio es el conjunto de parámetros y tal que[1]

1. $\mathfrak{A}$ asigna al símbolo de cuantificador $\forall$ un conjunto no vacío $|\mathfrak{A}|$ llamado el *universo* (o *dominio*) de $\mathfrak{A}$.
2. $\mathfrak{A}$ asigna a cada símbolo de predicado P de n argumentos una relación n-aria $P^{\mathfrak{A}} \subseteq |\mathfrak{A}|^n$; es decir, $P^{\mathfrak{A}}$ es un conjunto de n-adas de elementos del universo.
3. $\mathfrak{A}$ asigna a cada símbolo de constante c un elemento $c^{\mathfrak{A}}$ del universo $|\mathfrak{A}|$.
4. $\mathfrak{A}$ asigna a cada símbolo de función f de n argumentos una operación n-aria $f^{\mathfrak{A}}$ sobre $|\mathfrak{A}|$; es decir, $f^{\mathfrak{A}} : |\mathfrak{A}|^n \to |\mathfrak{A}|$.

La idea es que $\mathfrak{A}$ asigna significado a los parámetros. $\forall$ significa "para todo objeto de $|\mathfrak{A}|$". El símbolo c es para nombrar al punto $c^{\mathfrak{A}}$. La fórmula atómica $P t_1 \cdots t_n$ significa que la n-ada de puntos nombrados por $t_1, \ldots, t_n$ está en la relación $P^{\mathfrak{A}}$. (Pronto reformularemos estas condiciones con mayor cuidado.)

Nótese que requerimos que el universo $|\mathfrak{A}|$ sea no vacío. Nótese también que $f^{\mathfrak{A}}$ deberá tener la totalidad de $|\mathfrak{A}|^n$ como su

[1] El símbolo "$\mathfrak{A}$" es la letra A del alfabeto alemán (Fraktur). Las siguientes dos letras son $\mathfrak{B}$ y $\mathfrak{C}$.

dominio; no hemos hecho estipulación alguna para funciones parcialmente definidas.

EJEMPLO Considere el lenguaje de la teoría de conjuntos, cuyo único parámetro (además de $\forall$) es $\in$. Tome la estructura $\mathfrak{A}$ con

$|\mathfrak{A}|$ = el conjunto de los números naturales,
$\in^{\mathfrak{A}}$ = el conjunto de los pares $\langle m, n\rangle$ tal que $m < n$.

(Entonces, traducimos $\in$ como "es menor que"). En presencia de una estructura, podemos traducir enunciados del lenguaje formal al español e intentar decir si estas traducciones son verdaderas o falsas. El enunciado de este lenguaje de primer orden

$$\exists x \forall y \neg y \in x$$

(o más formalmente, $(\neg \forall v_1 (\neg \forall v_2 (\neg \in v_2 v_1))))$, que con otra traducción afirma la existencia de un conjunto vacío, se traduce ahora con $\mathfrak{A}$ como

Existe un número natural tal que ningún número natural es menor que él,

lo cual es verdad. Debido a esto, diremos que $\exists x \forall y \neg y \in x$ es *verdadero* en $\mathfrak{A}$, o que $\mathfrak{A}$ es un *modelo* del enunciado. Por otra parte, $\mathfrak{A}$ no es modelo del axioma del par,

$$\forall x \forall y \exists z \forall t (t \in z \leftrightarrow t = x \vee t = y),$$

pues la traducción de este enunciado con $\mathfrak{A}$ es falsa. Ya que no hay número natural m tal que para cada n,

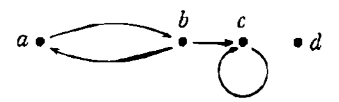
$$n < m \quad \text{sii} \quad n = 1.$$

(El lector que esté familiarizado con la teoría axiomática de conjuntos puede verificar que $\mathfrak{A}$ es un modelo del axioma de extensionalidad, del axioma de unión y del axioma de regularidad.)

Ejemplo De nuevo asuma que el lenguaje tiene únicamente los parámetros $\forall$ y un símbolo de predicado de dos argumentos E. Pero esta vez considere la estructura *finita* $\mathfrak{B}$ con universo $|\mathfrak{B}|$ que consiste en un conjunto de cuatro objetos distintos $\{a, b, c, d\}$. Suponga que la relación binaria $E^{\mathfrak{B}}$ es el siguiente conjunto de pares:

$$E^{\mathfrak{B}} = \{\langle a,b\rangle, \langle b, a\rangle, \langle b,c\rangle, \langle c,c\rangle\}.$$

Entonces podemos describir $\mathfrak{B}$ como la *gráfica dirigida* cuyo conjunto de vértices es el universo $\{a, b, c, d\}$:



Aquí, interpretamos Exy como si dijera que en la gráfica hay una *arista* del vértice x al vértice y. (Si la relación binaria $E^{\mathfrak{B}}$ hubiera sido simétrica, entonces podríamos haber descrito la estructura como una gráfica no dirigida.)

Considere ahora el enunciado $\exists x \forall y \neg yEx$. Con la estructura $\mathfrak{B}$ podemos traducirla como sigue:

> Existe un vértice tal que, para todo vértice, ninguna arista va del último al primero.

(¡La versión en español es más difícil de leer que la simbólica!) Este enunciado es verdadero en $\mathfrak{B}$ debido a que ninguna arista apunta al vértice d.

En los ejemplos anteriores fue intuitivamente claro que ciertos enunciados del lenguaje formal eran verdaderos en la estructura y otros eran falsos. Pero nosotros queremos una definición matemática precisa de "σ es verdadero en $\mathfrak{A}$". Esto deberá expresarse en términos matemáticos, sin emplear traducciones al español ni criterios supuestos para afirmar que algunos enunciados en español son verdaderos mientras que otros son falsos. (Si usted piensa que tiene tal criterio, póngalo a prueba con el enunciado "Este enunciado es falso".) En otras palabras, queremos tomar nuestro concepto informal "σ es verdadero en $\mathfrak{A}$" y hacerlo parte de las *matemáticas*.

Para definir "σ es verdadero en $\mathfrak{A}$",

$$\models_{\mathfrak{A}} \sigma,$$

para enunciados σ y estructuras $\mathfrak{A}$, lo deseable es definir primero un concepto más general relativo a las fórmulas. Sean

φ una fórmula de nuestro lenguaje,
$\mathfrak{A}$ una estructura para el lenguaje,
$s : V \to |\mathfrak{A}|$ una función del conjunto V de todas las variables, en el universo $|\mathfrak{A}|$ de $\mathfrak{A}$.

En seguida definiremos qué significa que $\mathfrak{A}$ *satisfaga* φ *con* s,

$$\models_{\mathfrak{A}} \varphi[s].$$

La versión informal es:

$\models_{\mathfrak{A}} \varphi[s]$ si y sólo si la traducción de φ determinada por $\mathfrak{A}$, donde la variable x se traduce como $s(x)$ en cualquier lugar en que ocurra libre, es verdadera.

La definición formal de satisfacción procede como sigue:

I. *Términos.* Definimos la extensión

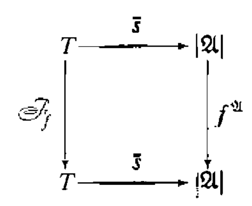
$$\bar{s} : T \to |\mathfrak{A}|,$$

una función del conjunto T de todos los términos, en el universo de $\mathfrak{A}$. La idea es que $\bar{s}(t)$ debería ser el elemento del universo $\mathfrak{A}$ que se nombra mediante el término t. $\bar{s}$ se define por recursión como sigue:

1. Para cada variable x, $\bar{s}(x) = s(x)$.
2. Para cada símbolo de constante c, $\bar{s}(c) = c^{\mathfrak{A}}$.
3. Si $t_1, \ldots, t_n$ son términos y f es un símbolo de función de n argumentos, entonces

$$\bar{s}(f t_1 \cdots t_n) = f^{\mathfrak{A}}(\bar{s}(t_1), \ldots, \bar{s}(t_n)).$$

Un diagrama conmutativo, para $n = 1$, es



La existencia de una única extensión $\bar{s}$ de s se sigue del teorema de recursión (Secc. 4, Cap. I), si se utiliza el dato de que los términos tienen descomposiciones únicas (sección 3 de este capítulo). Nótese que $\bar{s}$ depende tanto de s como de $\mathfrak{A}$. (De hecho, una notación alternativa razonable para $\bar{s}(t)$ sería $t^{\mathfrak{A}}[s]$, que manifiesta explícitamente la dependencia de $\mathfrak{A}$.)

II. *Fórmulas atómicas.* Las fórmulas atómicas se definieron explícitamente, no de manera inductiva. Por lo tanto, la definición de satisfacción de las fórmulas atómicas es también explícita y no recursiva.

1. $\models_{\mathfrak{A}} = t_1 t_2[s]$ sii $\bar{s}(t_1) = \bar{s}(t_2)$.

(Entonces, $=$ significa $=$. Nótese que $=$ es un símbolo lógico, no un parámetro sujeto a interpretación.)

2. Para un parámetro de predicado P de n argumentos,

$$\models_{\mathfrak{A}} Pt_1 \cdots t_n[s] \text{ sii } \langle \bar{s}(t_1), \ldots, \bar{s}(t_n) \rangle \in P^{\mathfrak{A}}.$$

III. *Otras fórmulas.* Las fórmulas que definimos por inducción; en consecuencia, aquí definiremos la satisfacción por recursión.

1. Para fórmulas atómicas, la definición está antes.
2. $\models_{\mathfrak{A}} \neg\varphi[s]$ sii $\not\models_{\mathfrak{A}} \varphi[s]$.
3. $\models_{\mathfrak{A}} (\varphi \rightarrow \psi)[s]$ sii o bien $\not\models_{\mathfrak{A}} \varphi[s]$, o bien $\models_{\mathfrak{A}} \psi[s]$, o ambos.

(En otras palabras, si $\mathfrak{A}$ satisface φ con s, entonces $\mathfrak{A}$ satisface ψ con s.)

4. $\models_{\mathfrak{A}} \forall x\, \varphi[s]$ sii para todo $d \in |\mathfrak{A}|$, tenemos:

$$\models_{\mathfrak{A}} \varphi[s(x \mid d)].$$

Aquí, $[s(x \mid d)]$ es la función exactamente como s, excepto que: en la variable x, toma el valor d. Esto se puede expresar mediante la ecuación

$$s(x|\,d)(y) = \begin{cases} s(y) & \text{si} \quad y \neq x, \\ d & \text{si} \quad y = x. \end{cases}$$

(Entonces $\forall$ significa "para todos los objetos de $|\mathfrak{A}|$".)

En este punto, es posible que el lector quiera reconsiderar la versión informal de $\models_{\mathfrak{A}} \varphi[s]$ de la página 125 y observar cómo fue formalizada.

Debemos hacer notar que la definición de satisfacción es otra aplicación del teorema de recursión junto con el hecho de que las fórmulas tienen descomposiciones únicas. La definición puede reformularse en términos de funciones para aclarar más cómo es que se aplica el teorema de recursión de la sección 4 del capítulo I.

(i) Consideremos una $\mathfrak{A}$ fija.

(ii) Definamos una función $\bar{h}$ (que extiende a una función h definida en las fórmulas atómicas) tal que para cualquier fórmula φ, $\bar{h}(\varphi)$ es un conjunto de funciones de V en $|\mathfrak{A}|$.

(iii) Definamos

$$\models_{\mathfrak{A}} \varphi[s] \quad \text{sii} \quad s \in \bar{h}(\varphi).$$

Dejamos al lector el ejercicio de escribir en detalle la definición explícita de h y las cláusulas que determinan de manera única su extensión $\bar{h}$. (Véase el ejercicio 7.) Una alternativa elegante es considerar que $\bar{h}(\varphi)$ es un conjunto de funciones en el conjunto de aquellas variables que ocurren libres en φ.

Ejemplo Suponga que nuestro lenguaje tiene los parámetros $\forall$, P (un símbolo de predicado de dos argumentos),

f (un símbolo de función de un argumento) y c (un símbolo de constante). Sea $\mathfrak{A}$ la estructura para este lenguaje definida como sigue:

$|\mathfrak{A}| = \mathbb{N}$, el conjunto de todos los números naturales,
$P^{\mathfrak{A}}$ = el conjunto de pares $\langle m, n\rangle$ tales que $m \leq n$,
$f^{\mathfrak{A}}$ = la función sucesor S; $f^{\mathfrak{A}}(n) = n + 1$,
$c^{\mathfrak{A}} = 0$.

Podemos resumir esto en una línea, suprimiendo el dato de que $\mathfrak{A}$ es en verdad una función y limitándonos a describir sus componentes:

$$\mathfrak{A} = (\mathbb{N}; \leq, S, 0).$$

Esta notación deja de ser ambigua únicamente cuando el contexto aclara exactamente qué componentes van con qué parámetros.

Sea $s : V \to \mathbb{N}$ la función para la cual $s(v_i) = i - 1$; es decir, $s(v_1) = 0$, $s(v_2) = 1$, y así sucesivamente.

1. $\bar{s}(ffv_3) = S(S(2)) = 4$ y $\bar{s}(fv_1) = S(0) = 1$.
2. $\bar{s}(c) = 0$ y $\bar{s}(ffc) = 2$; no se usa s.
3. $\models_{\mathfrak{A}} Pcfv_1[s]$. Esto es obvio informalmente, ya que cuando traducimos de nuevo al español, obtenemos el enunciado verdadero "$0 \leq 1$". Más formalmente, la razón es que

$$\langle \bar{s}(c), \bar{s}(fv_1)\rangle = \langle 0, 1\rangle \in P^{\mathfrak{A}}.$$

4. $\models_{\mathfrak{A}} \forall v_1 Pcv_1$. La traducción al español es "0 es menor o igual que cualquier número natural". Debemos verificar formalmente que para todo n en $\mathbb{N}$,

$$\models_{\mathfrak{A}} Pcv_1[s(v_1 \mid n)],$$

que se reduce a

$$\langle 0, n\rangle \in P^{\mathfrak{A}},$$

es decir, $0 \leq n$.

5. $\not\models_{\mathfrak{A}} \forall v_1 \; P v_2 v_1[s]$ porque existe un número natural m tal que

$$\not\models_{\mathfrak{A}} P v_2 v_1[s(v_1 \mid m)];$$

es decir,

$$\langle s(v_2), m\rangle \notin P^{\mathfrak{A}}.$$

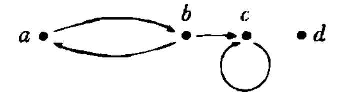
De hecho, ya que $s(v_2) = 1$, debemos tomar m como 0.

Se debe advertir al lector contra el riesgo de confundir, por ejemplo, el *símbolo* de función f con la *función* $f^{\mathfrak{A}}$.

Ejemplo Previamente habíamos considerado la estructura $\mathfrak{B}$ con

$$|\mathfrak{B}| = \{a, b, c, d\} \quad \text{y} \quad E^{\mathfrak{B}} = \{\langle a, b\rangle, \langle b, a\rangle, \langle b, c\rangle, \langle c, c\rangle\}$$

para el lenguaje con los parámetros $\forall$ y E:



Entonces, $\models_{\mathfrak{B}} \forall v_2 \neg E v_2 v_1[s]$ sii $s(v_1) = d$. Esto es, no hay arista que apunte al vértice d, pero d es el único vértice con esa condición. Tomando la negación de la fórmula, tenemos que $\models_{\mathfrak{B}} \exists v_2 E \, v_2 v_1[s]$ sii $s(v_1) \in \{a, b, c\}$.

En este punto hacemos una pausa para verificar que cuando queremos saber si la estructura $\mathfrak{A}$ satisface o no una fórmula φ con s, en realidad no necesitamos toda la (cantidad infinita de) información que nos da s. Todo lo que importa son los valores de la función s en (la cantidad finita de) variables que ocurren libres en φ. En particular, si φ es un enunciado, entonces s no importa en absoluto.

Teorema 22A Suponga que s_1 y s_2 son funciones de V en $|\mathfrak{A}|$ que coinciden en todas la variables que ocurren libres (si las hay) en la fórmula φ. Entonces

$$\models_{\mathfrak{A}} \varphi[s_1] \text{ sii } \models_{\mathfrak{A}} \varphi[s_2].$$

Demostración Debido a que la satisfacción se definió por recursión, esta prueba utiliza inducción. Consideramos la estructura fija $\mathfrak{A}$ y probamos por inducción que cada fórmula φ tiene la propiedad de que siempre que dos funciones s_1, s_2 coinciden en las variables libres en φ, entonces $\mathfrak{A}$ satisface φ con s_1 sii $\mathfrak{A}$ satisface φ con s_2.

Caso 1: $\varphi = Pt_1 \cdots t_n$ es atómica. Entonces, cualquier variable en φ ocurre libre. Por lo tanto, s_1 y s_2 coinciden en todas las variables en cada t_i. De esto se sigue que $\bar{s}_1(t_i) = \bar{s}_2(t_i)$ para cada i; una prueba detallada de esto utilizaría inducción sobre t_i. En consecuencia, $\mathfrak{A}$ satisface $Pt_1 \cdots t_n$ con s_1 sii $\mathfrak{A}$ satisface $Pt_1 \cdots t_n$ con s_2.

Casos 2 y 3: φ tiene la forma $\neg\alpha$ o $\alpha \rightarrow \beta$. Estos casos se siguen inmediatamente de la hipótesis inductiva.

Caso 4: $\varphi = \forall x\, \psi$. Entonces las variables libres en φ son aquellas libres en ψ con excepción de x. Por lo tanto, para cualquier d en $|\mathfrak{A}|$, $s_1(x\,|\,d)$ y $s_2(x\,|\,d)$ coinciden en todas las variables libres de ψ. Por hipótesis inductiva, entonces, $\mathfrak{A}$ satisface ψ con $s_1(x\,|\,d)$ sii $\mathfrak{A}$ satisface ψ con $s_2(x\,|\,d)$. A partir de esto y de la definición de satisfacción, vemos que $\mathfrak{A}$ satisface $\forall x\, \psi$ con s_1 sii $\mathfrak{A}$ satisface $\forall x\, \psi$ con s_2. ⊣

En efecto, la prueba anterior consiste en revisar la definición de satisfacción y observar qué información dada por s se utilizó realmente. Hay un hecho análogo referente a las estructuras: Si $\mathfrak{A}$ y $\mathfrak{B}$ coinciden en todos los parámetros que ocurren en φ, entonces $\models_{\mathfrak{A}} \varphi[s]$ sii $\models_{\mathfrak{B}} \varphi[s]$.

Este teorema justifica la siguiente notación: suponga que φ es una fórmula tal que todas las variables que ocurren libres en φ están incluidas entre $v_1, \ldots, v_k$. Entonces, para elementos $a_1, \ldots, a_k$ de $|\mathfrak{A}|$,

$$\models_{\mathfrak{A}} \varphi[[a_1, \ldots, a_k]]$$

significa que $\mathfrak{A}$ satisface φ con alguna (y por tanto con cualquier) función $s : V \rightarrow |\mathfrak{A}|$ para la cual $s(v_i) = a_i$, $1 \leq i \leq k$. Regresando a un ejemplo reciente en donde $\mathfrak{A} = (\mathbb{N}; \leq, S, 0)$, tenemos que $\models_{\mathfrak{A}} \forall v_2\, Pv_1v_2[[0]]$, pero $\not\models_{\mathfrak{A}} \forall v_2\, Pv_1v_2[[5]]$.

Corolario 22B Para un enunciado σ, o bien

(a) $\mathfrak{A}$ satisface σ con toda función s de V en $|\mathfrak{A}|$, o

(b) $\mathfrak{A}$ no satisface σ con cualquier función tal.

Si se cumple la alternativa (a), entonces decimos que σ es *verdadero* en $\mathfrak{A}$ (y se escribe $\models_{\mathfrak{A}} \sigma$) o que $\mathfrak{A}$ es un *modelo* de σ. Y si se cumple la alternativa (b), entonces por supuesto que σ es *falso* en $\mathfrak{A}$. (No se pueden cumplir ambas porque $|\mathfrak{A}|$ es no vacío.) $\mathfrak{A}$ es un *modelo* de un conjunto Σ de enunciados sii $\mathfrak{A}$ es un modelo de todos los elementos de Σ.

EJEMPLO Si $\mathfrak{R}$ es el campo de los reales, $(\mathbb{R}; 0, 1, +, \cdot)$, y $\mathfrak{Q}$ es el campo de los racionales, $(\mathbb{Q}; 0, 1, +, \cdot)$, ¿hay un enunciado que sea verdadero en uno y falso en el otro? Sí; debido a que $\sqrt{2}$ es irracional, el enunciado $\exists x (x \cdot x = 1 + 1)$ es falso en el campo de los racionales, pero verdadero en el campo de los reales.

EJEMPLO Suponga que nuestro lenguaje dado tiene sólo los parámetros $\forall$ y P, donde P es un símbolo de predicado de dos argumentos. Entonces una estructura $\mathfrak{A}$ queda determinada por el universo $|\mathfrak{A}|$ y la relación binaria $P^{\mathfrak{A}}$. Abusando ligeramente del lenguaje, escribimos de nuevo

$$\mathfrak{A} = (|\mathfrak{A}|; P^{\mathfrak{A}}).$$

Considere ahora el problema de caracterizar la clase de todos los modelos de los siguientes enunciados:

1. $\forall x \forall y\, x = y$. Una estructura $(A; R)$ es un modelo de este enunciado sii A tiene exactamente un elemento. R puede ser vacío o puede ser el conjunto unitario $A \times A$.

2. $\forall x \forall y\, Pxy$. Una estructura $(A; R)$ es un modelo de este enunciado sii $R = A \times A$. A puede ser cualquier conjunto no vacío.

3. $\forall x \forall y\, \neg Pxy$. Una estructura $(A; R)$ es un modelo de este enunciado sii $R = \emptyset$.

4. $\forall x\, \exists y\, Pxy$. La condición para que $(A; R)$ sea modelo de este enunciado es que el dominio de R sea A.

Las convenciones de notación hechas anteriormente se hicieron de modo racional:

1. $\models_{\mathfrak{A}} (\alpha \wedge \beta)[s]$ sii $\models_{\mathfrak{A}} \alpha[s]$ y $\models_{\mathfrak{A}} \beta[s]$; de manera similar para $\vee$ y $\leftrightarrow$.

2. $\models_{\mathfrak{A}} \exists x\, \alpha[s]$ sii hay algún $d \in |\mathfrak{A}|$ tal que $\models_{\mathfrak{A}} \alpha[s(x\,|\,d)]$.

La demostración para el segundo de éstos es como sigue:

$\models_{\mathfrak{A}} \exists x\, \alpha[s]$ sii $\models_{\mathfrak{A}} \neg\forall x \neg \alpha[s]$,
sii $\not\models_{\mathfrak{A}} \forall x \neg \alpha[s]$,
sii no es el caso de que para todo d en $|\mathfrak{A}|$, $\models_{\mathfrak{A}} \neg \alpha[s(x\,|\,d)]$,
sii no es el caso de que para todo d en $|\mathfrak{A}|$, $\not\models_{\mathfrak{A}} \alpha[s(x\,|\,d)]$,
sii para algún d en $|\mathfrak{A}|$, $\models_{\mathfrak{A}} \alpha[s(x\,|\,d)]$.

Implicación lógica

Ahora contamos con las herramientas necesarias para formular el importante concepto de implicación lógica para nuestro lenguaje.

Definición Sean Γ un conjunto de fórmulas y φ una fórmula. Entonces Γ ***implica lógicamente*** a φ, y se escribe $\Gamma \models \varphi$, sii para cada estructura $\mathfrak{A}$ del lenguaje y cada función $s : V \to |\mathfrak{A}|$ tal que $\mathfrak{A}$ satisface a cada elemento de Γ con s, $\mathfrak{A}$ también satisface a φ con s.

Utilizamos el mismo símbolo, "$\models$", que se utilizó en el capítulo I para la implicación tautológica. Pero de aquí en adelante se utilizará solamente para la implicación lógica. Al igual que antes, escribiremos "$\gamma \models \varphi$" en lugar de "$\{\gamma\} \models \varphi$". Decimos que φ y ψ son *lógicamente equivalentes* ($\varphi \models\dashv \psi$) sii $\varphi \models \psi$ y $\psi \models \varphi$.

El análogo en primer orden del concepto de tautología es el concepto de fórmula válida: una fórmula φ es *válida* sii $\emptyset \models \varphi$ (escrito simplemente como "$\models \varphi$"). Entonces, φ es válida sii para cada $\mathfrak{A}$ y cada $s : V \to |\mathfrak{A}|$, $\mathfrak{A}$ satisface φ con s.

Para enunciados, se puede establecer de modo más conciso el concepto de implicación lógica mediante la aplicación del teorema 22A:

Corolario 22C Para un conjunto $\Sigma; \tau$ de enunciados, $\Sigma \models \tau$ sii cada modelo de Σ es también modelo de τ. Un enunciado τ es válido sii es verdadero en todas las estructuras.

Ejemplos de implicación lógica. Se invita a los lectores a convencerse por sí mismos de lo siguiente:

1. $\forall v_1\ Qv_1 \models Qv_2$.

2. $Qv_1 \not\models \forall v_1\ Qv_1$. Aquí basta encontrar una sola estructura $\mathfrak{A}$ y una sola función $s : V \to |\mathfrak{A}|$ tal que, por una parte, $\models_{\mathfrak{A}} Qv_1[s]$ pero, por la otra, $\mathfrak{A}$ no es modelo de $\forall v_1\ Qv_1$. $|\mathfrak{A}|$ necesitará tener al menos dos elementos.

3. $\models \neg\neg\sigma \to \sigma$. Si $\mathfrak{A}$ es un modelo de $\neg\neg\sigma$, entonces $\not\models_{\mathfrak{A}} \neg\sigma$ de donde $\models_{\mathfrak{A}} \sigma$. Pero podríamos manifestar la siguiente objeción: ¿acaso no estamos *utilizando* aquí la ley de la doble negación, la ley que estamos pretendiendo probar? La respuesta es definitivamente sí y no. Estamos probando la ley de la doble negación para el lenguaje formal que nos ocupa (denominado a veces *el lenguaje objeto*). Al hacerlo, podemos utilizar, por supuesto, cualquier razonamiento correcto (afuera en el metalenguaje, el español), exactamente tal como lo haríamos al razonar respecto de espacios vectoriales o gráficas. En particular, el razonamiento puede implicar principios que cuando *se modelaran* formalmente, implicarían $\neg\neg\sigma$ y σ. No hay circularidad; pero los enunciados del metalenguaje que utilizamos —como era de esparar— están relacionados con las fórmulas del lenguaje objeto de las que hablamos. En conexión con esto, véase la única ilustración del libro (al final de la sección 4 de este capítulo).

4. $\forall v_1\ Qv_1 \models \exists v_2\ Qv_2$. Recuerde que el universo de cualquier estructura es no vacío.

5. $\exists x\ \forall y\ Pxy \models \forall y\ \exists x\ Pxy$. Este ejemplo volverá a aparecer en la sección 4 de este capítulo.

6. $\forall y \, \exists x \, Pxy \not\models \exists x \forall y \, Pxy$.

7. $\models \exists x (Qx \to \forall x \, Qx)$. Éste es un enunciado extraño, pero válido.

La definición de implicación lógica es muy parecida a la de implicación tautológica que aparece en el capítulo I; sin embargo, hay una diferencia importante en cuanto a su complejidad. Supongamos que en lógica de enunciados queremos saber si una fórmula α es una tautología o no. La definición requiere que consideremos un número finito de asignaciones de verdad, cada una de las cuales es una función finita. Para cada una de tales asignaciones de verdad v, debemos calcular $\overline{v}(\alpha)$, que puede realizarse efectivamente en una cantidad de tiempo finita. (En consecuencia, el conjunto de tautologías es decidible, como se observó anteriormente.)

En contraste con el procedimiento finitario para las tautologías, supongamos que queremos saber si una fórmula φ (de nuestro lenguaje de primer orden) es o no válida. La definición exige que consideremos cada estructura $\mathfrak{A}$. (En particular, esto requiere utilizar todos los conjuntos no vacíos, de los cuales hay una gran cantidad.) Para cada una de estas estructuras tenemos entonces que considerar cada función s del conjunto V de las variables en $|\mathfrak{A}|$. Y para cada $\mathfrak{A}$ y s dadas, debemos determinar si $\mathfrak{A}$ satisface φ con s o no. Cuando $|\mathfrak{A}|$ es infinito, ésta resulta en sí misma una noción complicada.

En vista de estas complicaciones, no es de sorprender que el conjunto de fórmulas válidas no sea decidible (compárese con la sección 5 del capítulo III). Lo que sí es sorprendente es que el concepto de validez resulta equivalente a otro concepto (deducibilidad) cuya definición es mucho más cercana a ser finitaria. (Véase la sección 4 de este capítulo.) Al utilizar esa equivalencia seremos capaces de probar (adoptando ciertas suposiciones razonables) que el conjunto de fórmulas válidas es efectivamente enumerable. El procedimiento de enumeración efectiva proporciona una caracterización más concreta del conjunto de las fórmulas válidas.

Definibilidad en una estructura

Supongamos que queremos estudiar el campo de los reales $(\mathbb{R}; 0, 1, +, \cdot)$ compuesto por el conjunto $\mathbb{R}$ de los números reales, junto con los elementos distinguidos 0 y 1 y las dos operaciones de suma y producto. Podemos considerar el campo de los reales como una estructura

$$\mathfrak{R} = (\mathbb{R}; 0, 1, +, \cdot)$$

en la que el lenguaje (con igualdad) tiene los símbolos de constante $\mathbf{0}$ y $\mathbf{1}$ y los símbolos de función de dos argumentos $\mathbf{+}$ y $\mathbf{\cdot}$.

Aunque no hemos incluido en el lenguaje un símbolo de orden $<$, aún tenemos una manera para decir "$x \geq 0$". Ya que, *en esta estructura*, los elementos no negativos son exactamente los elementos con raíces cuadradas. Esto es, la fórmula $\exists \mathbf{v}_2\, x = \mathbf{v}_2 \cdot \mathbf{v}_2$ se satisface en la estructura $\mathfrak{R}$ siempre que se asigne a x un número no negativo, y sólo en ese caso:

$$\models_{\mathfrak{R}} \exists \mathbf{v}_2\, \mathbf{v}_1 = \mathbf{v}_2 \cdot \mathbf{v}_2[[a]] \iff a \geq 0.$$

Debido a esto, diremos que el intervalo $[0, \infty)$ *es definible* en $\mathfrak{R}$, y que la fórmula $\exists \mathbf{v}_2\, \mathbf{v}_1 = \mathbf{v}_2 \cdot \mathbf{v}_2$ lo define.

Asimismo, la relación de orden en los reales, es decir, la relación binaria

$$\{\langle a, b\rangle \in \mathbb{R} \times \mathbb{R} \mid a \leq b\},$$

se define en la estructura $\mathfrak{R}$ mediante la fórmula que expresa "$\mathbf{v}_1 \leq \mathbf{v}_2$":

$$\exists \mathbf{v}_3\, \mathbf{v}_2 = \mathbf{v}_1 + \mathbf{v}_3 \cdot \mathbf{v}_3.$$

Para un ejemplo más corto, tómese la gráfica dirigida

$$\mathfrak{A} = (\{a, b, c\}; \{\langle a,b\rangle, \langle a,c\rangle\})$$

donde el lenguaje tiene los parámetros $\forall$ y E:

$$b \bullet \leftarrow \overset{a}{\bullet} \rightarrow \bullet\, c$$

Entonces en $\mathfrak{A}$, el conjunto $\{b, c\}$ (el rango o imagen de la relación $E^{\mathfrak{A}}$) se define mediante la fórmula $\exists \mathbf{v}_2\, E\mathbf{v}_2\mathbf{v}_1$. En cambio,

el conjunto $\{b\}$, *no* es definible en $\mathfrak{A}$. Esto se debe a que no hay propiedad definible en la estructura que separaría a b y c; la prueba de este hecho utilizará el teorema del homomorfismo, que se demostrará más adelante en esta sección.

Ahora queremos establecer de manera precisa este concepto de definibilidad de un subconjunto del universo o de una relación en el universo. Consideremos una estructura $\mathfrak{A}$ y una fórmula φ cuyas variables libres se encuentren entre $v_1, \ldots, v_k$. Entonces podemos construir sobre $|\mathfrak{A}|$ la relación de aridad k

$$\{\langle a_1, \ldots, a_k\rangle \mid \models_{\mathfrak{A}} \varphi[\![a_1, \ldots, a_k]\!]\}.$$

Llamemos a este conjunto la relación de aridad k que φ *define* en $\mathfrak{A}$. En general, se dice que una relación de aridad k sobre $|\mathfrak{A}|$ es *definible* en $\mathfrak{A}$ sii existe una fórmula (cuyas variables libres se encuentran entre $v_1, \ldots, v_k$) que la define ahí.

EJEMPLO Supongamos que tenemos una parte del lenguaje para la teoría de los números, específicamente que nuestro lenguaje tiene los parámetros $\forall$, **0**, **S**, **+** y **·**. Sea $\mathfrak{N}$ la estructura supuesta:

$|\mathfrak{N}| = \mathbb{N}$, el conjunto de los números naturales.
$\mathbf{0}^{\mathfrak{N}} = 0$, el número 0.
$\mathbf{S}^{\mathfrak{N}}$, $+^{\mathfrak{N}}$ y $\cdot^{\mathfrak{N}}$ son S, $+$ y $\cdot$, las funciones sucesor, suma y producto.

Expresado en una ecuación,

$$\mathfrak{N} = (\mathbb{N}; 0, S, +, \cdot).$$

Algunas relaciones sobre $\mathbb{N}$ son definibles en $\mathfrak{N}$ y otras no. Una manera de demostrar que algunas no son definibles es usar el dato de que hay una cantidad no numerable de relaciones sobre $\mathbb{N}$, pero únicamente una cantidad numerable de posibles fórmulas definitorias. (De cualquier modo, hay una dificultad inherente para dar un ejemplo específico. Después de todo, si algo es indefinible, ¡entonces es difícil decir qué es exactamente! Más adelante podremos ver un ejemplo específico, el conjunto de los números gödelianos de enunciados verdaderos en $\mathfrak{N}$; véase la sección 5 del capítulo III.)

1. La relación de orden $\{\langle m, n\rangle \mid m < n\}$ se define en $\mathfrak{N}$ mediante la fórmula

$$\exists v_3\, v_1 + \mathbf{S}\, v_3 = v_2.$$

2. Para cualquier número natural n, $\{n\}$ es definible. Por ejemplo, $\{2\}$ se define mediante la ecuación

$$v_1 = \mathbf{SS0}.$$

Por lo anterior, decimos que n es un *elemento definible* en $\mathfrak{N}$.

3. El conjunto de los primos es definible en $\mathfrak{N}$. Podemos utilizar la fórmula

$$\mathbf{1} < v_1 \wedge \forall v_2\, \forall v_3\, (v_1 = v_2 \cdot v_3 \rightarrow v_2 = \mathbf{1} \vee v_3 = \mathbf{1})$$

si tuviéramos los parámetros $\mathbf{1}$ y $<$ para 1 y $<$. Pero ya que $\{1\}$ y $<$ son definibles en $\mathfrak{N}$, realmente no hace falta agregar parámetros para ellos; en lugar de hacerlo, simplemente podemos usar sus definiciones. Entonces, el conjunto de primos es definible por

$$\exists v_3\, \mathbf{S0} + \mathbf{S}\, v_3 = v_1 \wedge \forall v_2\, \forall v_3 (v_1 = v_2 \cdot v_3 \rightarrow$$
$$v_2 = \mathbf{S0} \vee v_3 = \mathbf{S0}).$$

4. La exponenciación $\{\langle m, n, p\rangle \mid p = m^n\}$ también es definible en $\mathfrak{N}$. Esto de ningún modo es obvio; daremos una prueba más tarde (en la sección 8 del capítulo III) usando el teorema chino del residuo.

De hecho, discutiremos más adelante que cualquier relación decidible sobre $\mathbb{N}$ es definible en $\mathfrak{N}$, como lo son cualquier relación efectivamente numerable y muchas otras más. Hasta cierto punto se puede medir la complejidad de una relación definible mediante la complejidad de la fórmula definitoria más simple. Esta idea volverá a aparecer al final de la sección 5 del capítulo III.

Definibilidad de una clase de estructuras

En muchos cursos de matemáticas, el primer día el instructor comienza diciendo algo parecido a alguna de las siguientes afirmaciones:

1. "Una *gráfica* está compuesta, por definición, de un conjunto no vacío V junto con un conjunto E, tal que..."
2. "Un *grupo* está compuesto, por definición, de un conjunto no vacío G junto con una operación binaria $\circ$ que satisface los axiomas..."
3. "Un *campo ordenado* está compuesto, por definición, de un conjunto no vacío F junto con dos operaciones binarias $+$ y $\cdot$, y una relación binaria $<$ que satisface los axiomas..."
4. "Un *espacio vectorial* se compone, por definición, de un conjunto no vacío V junto con una operación binaria $+$ y, para cada número real r, una operación llamada multiplicación escalar tal que..."

Queremos hacer una abstracción de esta situación. En cada caso, los objetos de estudio (las gráficas, los grupos y los otros ejemplos) son *estructuras* para un lenguaje adecuado. Además, se exige que satisfagan un determinado conjunto Σ de enunciados (denominados "axiomas"). Posteriormente, el curso en cuestión estudia los modelos del conjunto Σ de axiomas, o al menos algunos de los modelos.

Para un conjunto Σ de enunciados, sea Mod Σ la clase de todos los modelos de Σ, es decir, la clase de todas las estructuras del lenguaje en las cuales todo elemento de Σ es verdadero. Para un solo enunciado τ simplemente escribimos "Mod τ" en lugar de "Mod $\{\tau\}$". (El lector familiarizado con la teoría axiomática de conjuntos, notará que si Mod Σ es no vacío, es una clase propia; es decir, es demasiado grande para ser un conjunto.)

Una clase $\mathcal{K}$ de estructuras de nuestro lenguaje es una *clase elemental* (EC) sii $\mathcal{K} = \text{Mod}\,\tau$ para algún enunciado τ. $\mathcal{K}$ es una *clase elemental en sentido amplio* (EC_Δ) sii $\mathcal{K} = \text{Mod}\,\Sigma$ para algún conjunto Σ de enunciados. (El adjetivo "elemental" se utiliza aquí como sinónimo de "primer orden".)

EJEMPLOS

1. Supongamos que el lenguaje cuenta con igualdad y dos parámetros $\forall$ y E, donde E es un símbolo de predicado de dos argumentos. Entonces una *gráfica* es una estructura para este lenguaje $\mathfrak{A} = (V; E^{\mathfrak{A}})$ consistente en un conjunto V no vacío de objetos llamados *vértices* (o *nodos*), y una *relación arista* $E^{\mathfrak{A}}$ que es simétrica (si $u\,E^{\mathfrak{A}}v$, entonces $v\,E^{\mathfrak{A}}u$) y antirreflexiva (nunca $v\,E^{\mathfrak{A}}v$). El axioma que manifiesta que la relación arista es simétrica y antirreflexiva se puede traducir mediante el enunciado

$$\forall x(\neg x E x \wedge \forall y(x E y \rightarrow y E x)).$$

Así, la clase de todas las gráficas es una clase elemental. Para *gráficas dirigidas* o *digráficas*, hacemos a un lado la suposición de simetría. Y si queremos permitir "rizos", entonces prescindimos de la suposición de antirreflexión. Pero tal vez ahora el instructor explique que en el curso únicamente se estudiarán las gráficas *finitas*. ¿Es la clase de todas las gráficas finitas una clase elemental? No, más adelante demostraremos que no lo es, ni siquiera en el sentido amplio.

2. Suponga que el lenguaje tiene igualdad y los parámetros $\forall$ y P, donde P es un símbolo de predicado de dos argumentos. Al igual que antes, una estructura $(A; R)$ para este lenguaje consiste en un conjunto A no vacío junto con una relación binaria R sobre A. $(A; R)$ se denomina un *conjunto ordenado* sii R es transitiva y satisface la condición de tricotomía (que dice que para cualesquiera a y b en A, se cumple exactamente una de las tres condiciones: $\langle a, b\rangle \in R$, $a = b$, $\langle b, a\rangle \in R$). Ya que éstas pueden traducirse como un enunciado del lenguaje formal, la clase de los conjuntos ordenados no vacíos es una clase elemental. Es, de hecho, Mod τ, donde τ es la conjunción de los tres enunciados

$$\forall x \forall y \forall z(xPy \rightarrow yPz \rightarrow xPz);$$
$$\forall x \forall y(xPy \vee x = y \vee yPx);$$
$$\forall x \forall y(xPy \rightarrow \neg yPx).$$

Los dos ejemplos siguientes suponen que el lector tiene alguna experiencia con álgebra.

3. Suponga que el lenguaje tiene = y los parámetros $\forall$ y $\circ$, donde $\circ$ es un símbolo de función de dos argumentos. La clase de todos los grupos es una clase elemental, y es la clase de todos los modelos de la conjunción de los axiomas de grupo:

$$\forall x \forall y \forall z\, (x \circ y) \circ z = x \circ (y \circ z);$$
$$\forall x \forall y \exists z\, x \circ z = y;$$
$$\forall x \forall y \exists z\, z \circ x = y.$$

La clase de todos los grupos infinitos es EC_Δ. Para ver esto, sea

$$\lambda_2 = \exists x \exists y\, x \neq y,$$
$$\lambda_3 = \exists x \exists y \exists z (x \neq y \wedge x \neq z \wedge y \neq z),$$
$$\ldots.$$

Por lo tanto, λ_n se traduce como "Existen al menos n cosas". Luego, el grupo de axiomas junto con $\{\lambda_2, \lambda_3, \ldots\}$ forman el conjunto Σ para el cual Mod Σ es exactamente la clase de los grupos infinitos. Finalmente nos será posible demostrar (en la sección 6 de este capítulo), que la clase de los grupos infinitos no es EC.

4. Suponga que el lenguaje tiene igualdad y los parámetros $\forall$, 0, 1, +, $\cdot$. Los campos pueden ser considerados como estructuras para este lenguaje. La clase de todos los campos es una clase elemental. La clase de los campos de característica cero es EC_Δ. No es EC; esto se sigue del teorema de compacidad para la lógica de primer orden (sección 6 de este capítulo).

Homomorfismos[2]

En cursos sobre gráficas, grupos o espacios vectoriales, normalmente uno encuentra el concepto de lo que significa que

[2] El estudio de este tema puede posponerse un poco; pero los homomorfismos se usarán en la comprobación del teorema de completud (con igualdad). Haremos uso del concepto de isomorfismo a partir de la sección 6 de este capítulo.

dos de las estructuras en cuestión, $\mathfrak{A}$ y $\mathfrak{B}$, sean *isomorfas*: en términos generales, debe haber una correspondencia uno a uno entre sus universos $|\mathfrak{A}|$ y $|\mathfrak{B}|$ que "preserve" las operaciones y las relaciones.

A continuación se explica que dos estructuras isomorfas, aunque no sean idénticas, deben tener las mismas propiedades matemáticas. Queremos definir aquí el concepto de isomorfismo en un contexto general, y mostrar que dos estructuras isomorfas tienen que satisfacer exactamente los mismos enunciados.

Sean $\mathfrak{A}$, $\mathfrak{B}$ estructuras para el lenguaje. Un *homomorfismo h* de $\mathfrak{A}$ en $\mathfrak{B}$ es una función $h : |\mathfrak{A}| \to |\mathfrak{B}|$ con las propiedades:

(a) Para cada parámetro de predicado P de n argumentos y cada n-ada $\langle a_1, \ldots, a_n \rangle$ de elementos de $|\mathfrak{A}|$,

$$\langle a_1, \ldots, a_n \rangle \in P^{\mathfrak{A}} \quad \text{sii} \quad \langle h(a_1), \ldots, h(a_n) \rangle \in P^{\mathfrak{B}}.$$

(b) Para cada símbolo de función f de n argumentos y para cada n-ada como antes,

$$h(f^{\mathfrak{A}}(a_1, \ldots, a_n)) = f^{\mathfrak{B}}(h(a_1), \ldots, h(a_n)).$$

En el caso de un símbolo de constante c, esto se convierte en

$$h(c^{\mathfrak{A}}) = c^{\mathfrak{B}}.$$

Las condiciones (a) y (b) se expresan normalmente como: "h preserva las relaciones y las funciones". (Hay que admitir que algunos autores utilizan una versión más débil de la condición (a); nuestros homomorfismos son sus "homomorfismos fuertes".)

Si, además, h es uno a uno, entonces se le llama un *isomorfismo* (o *inmersión isomorfa*) de $\mathfrak{A}$ en $\mathfrak{B}$. Si hay un isomorfismo de $\mathfrak{A}$ sobre $\mathfrak{B}$ (es decir, un isomorfismo h para el cual $\operatorname{ran} h = |\mathfrak{B}|$), entonces se dice que A y B son *isomorfas* (y se escribe $\mathfrak{A} \cong \mathfrak{B}$).

Es muy posible que el lector haya encontrado antes este concepto en ciertos casos especiales; por ejemplo, en las estructuras que son grupos o campos.

EJEMPLO Suponga que tenemos un lenguaje con los parámetros $\forall$, $+$, $\cdot$. Sea $\mathfrak{A}$ la estructura $(\mathbb{N}; +, \cdot)$. Podemos definir una función $h : \mathbb{N} \to \{e, o\}$ mediante

$$h(n) = \begin{cases} e & \text{si } n \text{ es par,} \\ o & \text{si } n \text{ es impar.} \end{cases}$$

Entonces, h es un homomorfismo de $\mathfrak{A}$ sobre $\mathfrak{B}$, donde $|\mathfrak{B}| = \{e, o\}$ y $+^{\mathfrak{B}}$, $\cdot^{\mathfrak{B}}$ se obtienen mediante las tablas siguientes:

$+^{\mathfrak{B}}$	e	o
e	e	o
o	o	e

$\cdot^{\mathfrak{B}}$	e	o
e	e	e
o	e	o

Se puede verificar que se satisface la condición (b) de la definición. Por ejemplo, si a y b son ambos números impares, entonces $h(a + b) = e$ y $h(a) +^{\mathfrak{B}} h(b) = o +^{\mathfrak{B}} o = e$.

EJEMPLO Sea $\mathbb{P}$ el conjunto de los enteros positivos, sea $<_P$ la relación de orden usual en $\mathbb{P}$, y sea $<_N$ la relación de orden usual en $\mathbb{N}$. Entonces existe un isomorfismo h de la estructura $(\mathbb{P}; <_P)$ sobre $(\mathbb{N}; <_N)$; tomamos $h(n) = n - 1$. También la función identidad $Id : \mathbb{P} \to \mathbb{N}$ es un isomorfismo de $(\mathbb{P}; <_P)$ en $(\mathbb{N}; <_N)$. Debido a este último hecho, decimos que $(\mathbb{P}; <_P)$ es una *subestructura* de $(\mathbb{N}; <_N)$.

De una forma más general, consideremos dos estructuras $\mathfrak{A}$ y $\mathfrak{B}$ para el lenguaje, tales que $|\mathfrak{A}| \subseteq |\mathfrak{B}|$. A partir de la definición de homomorfismo, está claro que la función identidad de $|\mathfrak{A}|$ en $|\mathfrak{B}|$ es un isomorfismo de $\mathfrak{A}$ en $\mathfrak{B}$ sii

(a) $P^{\mathfrak{A}}$ es la restricción de $P^{\mathfrak{B}}$ a $|\mathfrak{A}|$, para cada parámetro de predicado P;

(b) $f^{\mathfrak{A}}$ es la restricción de $f^{\mathfrak{B}}$ a $|\mathfrak{A}|$, para cada símbolo de función f, y $c^{\mathfrak{A}} = c^{\mathfrak{B}}$, para cada símbolo de constante c.

Si se cumplen estas condiciones, entonces se dice que $\mathfrak{A}$ es una *subestructura* de $\mathfrak{B}$ y que $\mathfrak{B}$ es una *extensión* de $\mathfrak{A}$.

Por ejemplo, en un lenguaje con un símbolo de función de dos argumentos $+$, la estructura $(\mathbb{Q}; +_Q)$ es una subestructura de $(\mathbb{C}; +_C)$. Aquí, $+_C$ es la operación de suma para números complejos. Y $+_Q$, la suma para racionales, es exactamente la restricción de $+_C$ al conjunto $\mathbb{Q}$.

En este ejemplo, el conjunto $\mathbb{Q}$ es cerrado bajo $+_C$; esto es, la suma de dos números racionales es un racional. De una forma más general, siempre que $\mathfrak{A}$ sea una subestructura de $\mathfrak{B}$, entonces $|\mathfrak{A}|$ deberá ser cerrado bajo $f^{\mathfrak{B}}$ para cada símbolo de función f. Después de todo, $f^{\mathfrak{B}}(\vec{a})$ (donde $\vec{a} \in |\mathfrak{A}|^n$) no es otra cosa que $f^{\mathfrak{A}}(\vec{a})$, el cual debe ser algún elemento de $|\mathfrak{A}|$. Esta propiedad de cerradura se cumple incluso para los símbolos de función de 0 argumentos; así, $c^{\mathfrak{B}}$ debe pertenecer a $|\mathfrak{A}|$ para cada símbolo de constante c.

A la inversa, supongamos que tenemos una estructura $\mathfrak{B}$, y sea A un subconjunto no vacío de $|\mathfrak{B}|$ cerrado bajo todas las funciones de $\mathfrak{B}$, al igual que en el párrafo anterior. Entonces podemos hacer una subestructura de $\mathfrak{B}$ con universo A. De hecho, hay una sola manera de hacer esto. El universo es A, a cada parámetro de predicado P se le asigna la restricción de $P^{\mathfrak{B}}$ a A, y se hace lo mismo para los símbolos de función. Como un caso extremo, si el lenguaje no tiene símbolos de función (ni siquiera símbolos de constante), entonces podemos hacer una subestructura a partir de *cualquier* subconjunto A no vacío de $|\mathfrak{B}|$.

Éstos son básicamente conceptos algebraicos, pero el teorema siguiente los relaciona con los conceptos lógicos de verdad y de satisfacción.

Teorema del homomorfismo Sea h un homomorfismo de $\mathfrak{A}$ en $\mathfrak{B}$, y sea s una función del conjunto de las variables en $|\mathfrak{A}|$.

(a) Para cualquier término t tenemos $h(\bar{s}(t)) = \overline{h \circ s}(t)$, donde $\bar{s}(t)$ se calcula en $\mathfrak{A}$ y $\overline{h \circ s}(t)$ se calcula en $\mathfrak{B}$.

(b) Para cualquier fórmula α libre de cuantificadores que no contenga símbolo de igualdad,

$$\models_{\mathfrak{A}} \alpha[s] \quad \text{sii} \quad \models_{\mathfrak{B}} \alpha[h \circ s].$$

(c) Si h es uno a uno (es decir, es un isomorfismo de $\mathfrak{A}$ en $\mathfrak{B}$), entonces en la parte (b) podemos eliminar la restricción "no contenga símbolo de igualdad".

(d) Si h es un homomorfismo de $\mathfrak{A}$ *sobre* $\mathfrak{B}$, entonces en (b) podemos eliminar la restricción "libre de cuantificadores".

Demostración La parte (a) usa inducción sobre t; véase el ejercicio 13. Nótese que $h \circ s$ es una función del conjunto de las variables en $|\mathfrak{B}|$; su extensión al conjunto de todos los términos es $\overline{h \circ s}$. Es pues $\overline{h \circ s}$ la función que aquí se evalúa en t.

(b) Para una fórmula atómica tal como Pt, tenemos

$$\begin{aligned} \models_{\mathfrak{A}} Pt[s] &\Leftrightarrow \bar{s}(t) \in P^{\mathfrak{A}} \\ &\Leftrightarrow h(\bar{s}(t)) \in P^{\mathfrak{B}} && \text{ya que } h \text{ es un homomorfismo} \\ &\Leftrightarrow \overline{h \circ s}(t) \in P^{\mathfrak{B}} && \text{por (a)} \\ &\Leftrightarrow \models_{\mathfrak{B}} Pt[h \circ s]. \end{aligned}$$

Se requiere entonces un argumento inductivo para manejar el caso de los símbolos de conectivo $\neg$ y $\rightarrow$, pero es mera rutina.

(c) En cualquier caso,

$$\begin{aligned} \models_{\mathfrak{A}} u = t[s] &\Leftrightarrow \bar{s}(u) = \bar{s}(t) \\ &\Rightarrow h(\bar{s}(u)) = h(\bar{s}(t)) \\ &\Leftrightarrow \overline{h \circ s}(u) = \overline{h \circ s}(t) && \text{por (a)} \\ &\Leftrightarrow \models_{\mathfrak{B}} u = t[h \circ s]. \end{aligned}$$

Si h es uno a uno, entonces la flecha del segundo paso también se puede invertir.

(d) Debemos extender el argumento inductivo de rutina de la parte (b) para incluir el paso del cuantificador. Esto es, debemos mostrar que si φ tiene la propiedad de que para toda s,

$$\models_{\mathfrak{A}} \varphi[s] \Leftrightarrow \models_{\mathfrak{B}} \varphi[h \circ s],$$

entonces $\forall x \varphi$ tiene la misma propiedad. En todo caso (como una consecuencia de la hipótesis inductiva para φ) tenemos la implicación

$$\models_{\mathfrak{B}} \forall x\varphi[h \circ s] \Rightarrow \models_{\mathfrak{A}} \forall x\varphi[s].$$

De manera intuitiva, esto es muy plausible. Si φ es verdadero para todos los elementos en el conjunto más grande $|\mathfrak{B}|$, entonces es verdadero *a fortiori* para todos en el conjunto más pequeño ran h. Los detalles son, para un elemento a de $|\mathfrak{A}|$,

$$\models_{\mathfrak{B}} \forall x\varphi[h\circ s] \Rightarrow \models_{\mathfrak{B}} \varphi[(h \circ s)(x \mid h(a))]$$

$$\Leftrightarrow \models_{\mathfrak{B}} \varphi[h \circ (s(x \mid a))],$$ las funciones son las mismas

$$\Leftrightarrow \models_{\mathfrak{A}} \varphi[s(x \mid a)]$$ por la hipótesis inductiva.

Ahora para el inverso, suponga que $\not\models_{\mathfrak{B}} \forall x\varphi[h \circ s]$, de modo que $\models_{\mathfrak{B}} \neg\varphi[(h \circ s)(x \mid b)]$ para algún elemento b de $|\mathfrak{B}|$. Necesitamos la implicación

(*) *Si* para algún b de $|\mathfrak{B}|$, $\models_{\mathfrak{B}} \neg\varphi[(h\circ s)(x \mid b)]$, *entonces* para algún a de $|\mathfrak{A}|$, $\models_{\mathfrak{B}} \neg\varphi[(h \circ s)(x \mid h(a))]$.

Pues dado (*), podemos proceder:

$$\models_{\mathfrak{B}} \neg\varphi[(h\circ s)(x \mid h(a))] \Leftrightarrow \models_{\mathfrak{B}} \neg\varphi[h \circ (s(x \mid a))],$$ las funciones son las mismas

$$\Leftrightarrow \models_{\mathfrak{A}} \neg\varphi[s(x \mid a)]$$ por la hipótesis inductiva

$$\Rightarrow \not\models_{\mathfrak{A}} \forall x\varphi[s].$$

Si h es función de $|\mathfrak{A}|$ *sobre* $|\mathfrak{B}|$, entonces (*) es inmediato; tomamos a tal que $b = h(a)$. (Pero puede haber otras ocasiones afortunadas en que se puede afirmar (*) incluso si h no tiene rango $|\mathfrak{B}|$.) ⊣

Se dice que dos estructuras $\mathfrak{A}$ y $\mathfrak{B}$ son ***elementalmente equivalentes*** (se escribe $\mathfrak{A} \equiv \mathfrak{B}$) sii para cualquier enunciado σ,

$$\models_{\mathfrak{A}} \sigma \Leftrightarrow \models_{\mathfrak{B}} \sigma.$$

Corolario 22D Las estructuras isomorfas son elementalmente equivalentes:

$$\mathfrak{A} \cong \mathfrak{B} \Rightarrow \mathfrak{A} \equiv \mathfrak{B}$$

Realmente, hay más de cierto. Las estructuras isomorfas se parecen de cualquier manera "estructural"; no sólo satisfacen los mismos enunciados de primer orden, sino que también satisfacen los mismos enunciados de segundo orden (y de órdenes superiores), (es decir, son equivalentes en segundo orden y más).

Existen estructuras elementalmente equivalentes que no son isomorfas. Por ejemplo, se puede mostrar que la estructura $(\mathbb{R}; <_R)$ formada por el conjunto de los números reales con su relación de orden usual es elementalmente equivalente a la estructura $(\mathbb{Q}; <_Q)$, compuesta por el conjunto de los números racionales con su orden natural (véase la sección 6 de este capítulo). Pero $\mathbb{Q}$ es un conjunto numerable mientras que $\mathbb{R}$ no lo es, así que estas estructuras no pueden ser isomorfas. En la sección 6 veremos qué fácil es hacer estructuras elementalmente equivalentes de cardinalidades diferentes.

Ejemplo revisado. Vimos antes un isomorfismo h de $(\mathbb{P}; <_P)$ sobre $(\mathbb{N}; <_N)$. Así que, en particular, $(\mathbb{P}; <_P) \equiv (\mathbb{N}; <_N)$; estas estructuras son indistinguibles mediante enunciados de primer orden.

Incluso hicimos hincapié en que la función identidad era una inmersión isomorfa de $(\mathbb{P}; <_P)$ en $(\mathbb{N}; <_N)$. De aquí que para una función $s : V \to \mathbb{P}$ y para una φ libre de cuantificadores,

$$\models_{(\mathbb{P};<_P)} \varphi[s] \Leftrightarrow \models_{(\mathbb{N};<_N)} \varphi[s].$$

Esta equivalencia puede fallar si φ contiene cuantificadores. Por ejemplo,

$$\models_{(\mathbb{P};<_P)} \forall v_2(v_1 \neq v_2 \to v_1 < v_2)[[1]],$$

pero

$$\not\models_{(\mathbb{N};<_N)} \forall v_2(v_1 \neq v_2 \to v_1 < v_2)[[1]].$$

Un *automorfismo* de la estructura $\mathfrak{A}$ es un isomorfismo de $\mathfrak{A}$ sobre $\mathfrak{A}$. La función de identidad en $|\mathfrak{A}|$ es, trivialmente, un automorfismo de $\mathfrak{A}$. $\mathfrak{A}$ puede o no tener automorfismos no triviales. (Decimos que $\mathfrak{A}$ es *rígida* si la función de identidad es

su único automorfismo.) Como una consecuencia del teorema del homomorfismo, podemos mostrar que un automorfismo tiene que preservar las relaciones definibles:

Corolario 22E Sea h un automorfismo de la estructura $\mathfrak{A}$, y sea R una relación n-aria sobre $|\mathfrak{A}|$ definible en $\mathfrak{A}$. Entonces, para cualesquiera $a_1, \ldots, a_n$ en $|\mathfrak{A}|$,

$$\langle a_1, \ldots, a_n \rangle \in R \Leftrightarrow \langle h(a_1), \ldots, h(a_n) \rangle \in R.$$

Demostración Sea φ una fórmula que define R en $\mathfrak{A}$. Necesitamos saber que

$$\models_{\mathfrak{A}} \varphi[[a_1, \ldots, a_n]] \Leftrightarrow \models_{\mathfrak{A}} \varphi[[h(a_1), \ldots, h(a_n)]].$$

Pero esto es inmediato a partir del teorema del homomorfismo. ⊣

Este corolario es útil a veces para mostrar que una relación dada *no* es definible. Por ejemplo, considere la estructura $(\mathbb{R}; <)$ compuesta por el conjunto de los números reales con su orden usual. Un automorfismo de esta estructura es simplemente una función h de $\mathbb{R}$ sobre $\mathbb{R}$ que es estrictamente creciente:

$$a < b \Leftrightarrow h(a) < h(b).$$

Un automorfismo de ese estilo es la función h para la cual $h(a) = a^3$. Como esta función manda puntos de fuera de $\mathbb{N}$ a puntos dentro de $\mathbb{N}$, el conjunto $\mathbb{N}$ no es definible en esta estructura.

Otro ejemplo es el que proveen los libros de álgebra elemental, los cuales a veces explican que la longitud de un vector en el plano no puede ser definida en términos de suma de vectores y multiplicación escalar. La función que toma al vector $\mathbf{x}$ y lo lleva al vector $2\mathbf{x}$ es un automorfismo del plano con respecto a la suma de vectores y a la multiplicación escalar, pero no preserva la longitud. Desde nuestro punto de vista, la estructura en cuestión,

$$(E; +, f_r)_{r \in \mathbb{R}},$$

tiene al plano E como universo, tiene la operación binaria $+$ para la suma de vectores, y tiene (para cada r en el conjunto $\mathbb{R}$)

la operación unaria f_r de multiplicación escalar por r. (De este modo, el lenguaje en cuestión tiene un símbolo de función de un argumento para cada número real.) La función que duplica, descrita antes es un automorfismo de esta estructura. Pero no preserva el conjunto de vectores unitarios,

$$\{\mathbf{x} \mid \mathbf{x} \in \boldsymbol{E} \text{ y } \mathbf{x} \text{ tiene longitud } 1\}.$$

Así que este conjunto no puede ser definible en la estructura. (Por cierto, los homomorfismos de los espacios vectoriales se denominan *transformaciones lineales*.)

Ejercicios

1. Muestre que (a) $\Gamma; \alpha \models \varphi$ sii $\Gamma \models (\alpha \to \varphi)$; y (b) $\varphi \mathrel{\models\!\!\!\dashv} \psi$ sii $\models (\varphi \leftrightarrow \psi)$.
2. Muestre que ninguno de los enunciados siguientes está lógicamente implicado por los otros dos. (Esto se hace dando una estructura en la cual el enunciado en cuestión es falso, mientras que los otros dos son verdaderos.)
   (a) $\forall x \, \forall y \, \forall z \, (Pxy \to Pyz \to Pxz)$. Recuerde que según nuestra convención, $\alpha \to \beta \to \gamma$ es $\alpha \to (\beta \to \gamma)$.
   (b) $\forall x \, \forall y \, (Pxy \to Pyx \to x = y)$.
   (c) $\forall x \, \exists y \, Pxy \to \exists y \, \forall x \, Pxy$.
3. Muestre que
$$\{\forall x \, (\alpha \to \beta), \forall x \alpha\} \models \forall x \beta.$$
4. Muestre que si x no ocurre libre en α, entonces $\alpha \models \forall x \alpha$.
5. Muestre que la fórmula $x = y \to Pzfx \to Pzfy$ (donde f es un símbolo de función de un argumento y P es un símbolo de predicado de dos argumentos) es válida.
6. Muestre que una fórmula θ es válida sii $\forall x \theta$ es válida.
7. Reformule la definición de "$\mathfrak{A}$ satisface φ con s" de la manera descrita en la parte III de la definición de satisfacción (sección 2, pp. 126 y 127). Esto es, defina mediante recursión una función $\overline{h}$ tal que $\mathfrak{A}$ satisface φ con s sii $s \in \overline{h}(\varphi)$.

8. Supongamos que Σ es un conjunto de enunciados tal que para cualquier enunciado τ, o bien $\Sigma \models \tau$ o $\Sigma \models \neg\tau$. Supongamos que $\mathfrak{A}$ es un modelo de Σ. Muestre que para cualquier enunciado τ, tenemos que $\models_{\mathfrak{A}} \tau$ sii $\Sigma \models \tau$.

9. Supongamos que el lenguaje tiene igualdad y un símbolo de predicado P de dos argumentos. Para cada una de las condiciones siguientes, encuentre un enunciado σ tal que la estructura $\mathfrak{A}$ es un modelo de σ sii se cumple la condición.

   (a) $|\mathfrak{A}|$ tiene exactamente dos elementos.

   (b) $P^{\mathfrak{A}}$ es una función de $|\mathfrak{A}|$ en $|\mathfrak{A}|$. (Una *función* es una relación monovaluada, como en el capítulo cero. Para que f sea una función de A en B, el dominio de f debe ser la totalidad de A; el rango de f es un subconjunto no necesariamente propio de B.)

   (c) $P^{\mathfrak{A}}$ es una permutación de $|\mathfrak{A}|$; es decir, $P^{\mathfrak{A}}$ es una función uno a uno con dominio y rango igual a $|\mathfrak{A}|$.

10. Muestre que

$$\models_{\mathfrak{A}} \forall v_2\, Qv_1v_2[[c^{\mathfrak{A}}]] \quad \text{sii} \quad \models_{\mathfrak{A}} \forall v_2\, Qcv_2.$$

   Aquí Q es un símbolo de predicado de dos argumentos y c es un símbolo de constante.

11. Para cada una de las relaciones siguientes, dé una fórmula que la defina en $(\mathbb{N}; +, \cdot)$. (Se supone que el lenguaje tiene igualdad y cuenta con los parámetros $\forall$, $+$ y $\cdot$.)

   (a) $\{0\}$.

   (b) $\{1\}$.

   (c) $\{\langle m, n\rangle \mid n$ es el sucesor de m en $\mathbb{N}\}$.

   (d) $\{\langle m,n\rangle \mid m < n$ en $\mathbb{N}\}$.

   Digresión: Ésta no es más que la punta del iceberg. Se dice que una relación en $\mathbb{N}$ es *aritmética* si es definible en esta estructura. Todas las relaciones decidibles son aritméticas, al igual que muchas otras. Las relaciones aritméticas pueden ser dispuestas en una jerarquía; véase la sección 5 del capítulo III.

12. Sea $\mathfrak{R}$ la estructura $(\mathbb{R}; +, \cdot)$. (Se supone que el lenguaje tiene igualdad y los parámetros $\forall$, $+$ y $\cdot$. $\mathfrak{R}$ es la estructura cuyo universo es el conjunto $\mathbb{R}$ de los números reales y es tal que $+^{\mathfrak{R}}$ y $\cdot^{\mathfrak{R}}$ son las operaciones usuales de suma y producto.)
    (a) Dé una fórmula que defina en $\mathfrak{R}$ el intervalo $[0, \infty)$.
    (b) Dé una fórmula que defina en $\mathfrak{R}$ el conjunto $\{2\}$.
    *(c) Muestre que cualquier unión finita de intervalos cuyos extremos son algebraicos es definible en $\mathfrak{R}$. (El inverso también es verdadero; éstos son los únicos conjuntos definibles en la estructura. Pero no demostraremos este hecho.)

13. Demuestre la parte (a) del teorema del homomorfismo.

14. ¿Qué subconjuntos de la recta real $\mathbb{R}$ son definibles en $(\mathbb{R}; <)$? ¿Qué subconjuntos del plano $\mathbb{R} \times \mathbb{R}$ son definibles en $(\mathbb{R}; <)$?

    Comentarios: Lo bueno de $(\mathbb{R}; <)$ es que sus automorfismos son exactamente las funciones de $\mathbb{R}$ sobre sí mismo que preservan el orden. No obstante, nos detendremos después de las relaciones binarias, pues existen 2^{13} relaciones ternarias definibles, así que el lector no querrá catalogarlas todas.

15. Muestre que la relación de suma, $\{\langle m, n, p\rangle \mid p = m + n\}$, no es definible en $(\mathbb{N}; \cdot)$. *Sugerencia*: considere un automorfismo de $(\mathbb{N}; \cdot)$ que intercambie dos primos.

    Digresión: Desde el punto de vista algebraico, la estructura de los números naturales con multiplicación no es otra cosa que el semigrupo abeliano libre con $\aleph_0$ generadores (es decir, los primos), junto con un elemento cero. Aquí no hay manera de definir la suma; si se pudiera hacer, entonces podría definirse el orden (por el ejercicio 11 y por transitividad). Pero un generador se ve igual a otro. Esto es, hay $2^{\aleph_0}$ automorfismos —simplemente permute los primos. Ninguno de ellos preserva el orden excepto la identidad.

16. Escriba un enunciado que tenga modelos de tamaño $2n$ para cada entero positivo n, pero que no tenga modelos finitos de tamaño impar. (En este caso, el lenguaje deberá incluir igualdad y tendrá los parámetros que se quieran elegir.) *Sugerencia*: un método es formular un enunciado que diga "Todo objeto es o rojo o azul, y f es una permutación que invierte el color."

Comentario: Dado un enunciado σ, es posible que tenga algunos modelos finitos (es decir, modelos con universos finitos). Defina el *espectro* de σ para que sea el conjunto de enteros positivos n tal que σ tenga un modelo de tamaño n. Este ejercicio muestra que el conjunto de los números pares es un espectro.

Por ejemplo, si σ es la conjunción de los axiomas de campo (sólo hay una cantidad finita, así que podemos tomar su conjunción), entonces su espectro es el conjunto de potencias de los primos. Esto se prueba en cualquier curso de campos finitos. En cambio, el espectro de $\neg\sigma$ es el conjunto de todos los enteros positivos (los que no son campos se presentan en todos los tamaños).

En 1955, Günter Asser planteó la pregunta: ¿es un espectro el complemento de todo espectro? Una vez que nos demos cuenta de que tomar la negación simplemente no funciona (véase el párrafo precedente), veremos que ésta no es una pregunta trivial. De hecho, este problema, conocido como el problema del espectro, todavía no tiene solución. No obstante, el trabajo moderno lo ha vinculado con otro problema aún por resolver: si se cumple o no que co-NP = NP.

17. (a) Considere un lenguaje con igualdad cuyo único parámetro (además de $\forall$) es un símbolo de predicado P de dos argumentos. Muestre que si $\mathfrak{A}$ es finito y $\mathfrak{A} \equiv \mathfrak{B}$, entonces $\mathfrak{A}$ es isomorfa a $\mathfrak{B}$. *Sugerencia*: Suponga que el universo de $\mathfrak{A}$ tiene tamaño n. Construya un solo enunciado σ de la forma $\exists v_1 \cdots \exists v_n\, \theta$ que describa $\mathfrak{A}$ "completamente". Esto es, por una parte, σ deberá ser verdadero en $\mathfrak{A}$. Y, por la otra, cualquier modelo

de σ deberá ser exactamente como $\mathfrak{A}$ (es decir, isomorfo a $\mathfrak{A}$).

*(b) Muestre que el resultado de la parte (a) se mantiene, independientemente de los parámetros que contenga el lenguaje.

18. Una fórmula universal ($\forall_1$) tiene la forma $\forall x_1 \cdots \forall x_n\ \theta$, donde θ está libre de cuantificadores. Una fórmula existencial ($\exists_1$) es de la forma dual $\exists x_1 \cdots \exists x_n\ \theta$. Sea $\mathfrak{A}$ una subestructura de $\mathfrak{B}$ y sea $s : V \to |\mathfrak{A}|$.

(a) Muestre que si $\models_{\mathfrak{A}} \psi[s]$ y ψ es existencial, entonces $\models_{\mathfrak{B}} \psi[s]$. Y muestre que si $\models_{\mathfrak{B}} \varphi[s]$ y φ es universal, entonces $\models_{\mathfrak{A}} \varphi[s]$.

(b) Concluya que el enunciado $\exists x\ Px$ no es lógicamente equivalente a ningún enunciado universal, y que $\forall x\ Px$ tampoco lo es con respecto a ningún enunciado existencial.

Comentario: La parte (a) dice (cuando φ es un enunciado) que cualquier enunciado universal "se preserva bajo subestructuras". Ser universal es una propiedad sintáctica: tiene que ver con la cadena de símbolos. En cambio, ser preservado bajo subestructuras es una propiedad semántica: tiene que ver con la satisfacción en estructuras. Pero esta propiedad semántica captura a la propiedad sintáctica hasta la equivalencia lógica (que es todo lo que podríamos pedir). Esto es, si σ es un enunciado que siempre se preserva bajo subestructuras, entonces σ es lógicamente equivalente a un enunciado universal. (Este hallazgo se debe a Loś y Tarski.)

19. Una fórmula $\exists_2$ tiene la forma $\exists x_1 \cdots \exists x_n\ \theta$, donde θ es universal.

(a) Muestre que si un enunciado $\exists_2$ de un lenguaje que no contenga símbolos de función (ni siquiera símbolos de constante) es verdadero en $\mathfrak{A}$, entonces es verdadero en alguna subestructura finita de $\mathfrak{A}$.

(b) Concluya que $\forall x\ \exists y\ Pxy$ no es lógicamente equivalente a ningún enunciado $\exists_2$.

20. Supongamos que el lenguaje tiene igualdad y un símbolo de predicado P de dos argumentos. Considere las dos estructuras $(\mathbb{N}; <)$ y $(\mathbb{R}; <)$ para el lenguaje.

    (a) Encuentre un enunciado que sea verdadero en una estructura y falso en la otra.

    *(b) Muestre que cualquier enunciado $\exists_2$ (tal como se definió en el ejercicio anterior) verdadero en $(\mathbb{R}; <)$ también es verdadero en $(\mathbb{N}; <)$. *Sugerencia:* Primero, para cualquier conjunto finito de números reales, existe un automorfismo de $(\mathbb{R}; <)$ que lleva esos números reales a números naturales. Segundo, por el ejercicio 18, las fórmulas universales se preservan bajo subestructuras.

21. Podríamos considerar enriquecer el lenguaje agregando un nuevo símbolo de cuantificador. La fórmula $\exists! x\ \alpha$ (que se lee "existe una única x tal que α") se satisface en $\mathfrak{A}$ por s sii hay una y sólo una $a \in |\mathfrak{A}|$ tal que $\models_{\mathfrak{A}} \alpha[s(x\,|\,a)]$. Suponga que el lenguaje tiene el símbolo de igualdad y muestre que este aparente enriquecimiento no es tal, en el sentido de que podemos encontrar una fórmula ordinaria lógicamente equivalente a $\exists! x\ \alpha$.

22. Supongamos que $\mathfrak{A}$ es una estructura y que h es una función tal que ran $h = |\mathfrak{A}|$. Muestre que hay una estructura $\mathfrak{B}$ tal que h es un homomorfismo de $\mathfrak{B}$ sobre $\mathfrak{A}$. *Sugerencia:* Necesitamos tomar $|\mathfrak{B}| =$ dom h. En general, se necesitará del axioma de elección para definir las funciones en $\mathfrak{B}$, a menos que h sea uno a uno.

    Comentario: El resultado produce un "teorema ascendente de Löwenheim-Skolem sin igualdad" (véase la sección 6 de este capítulo). Esto es, cualquier estructura $\mathfrak{A}$ tiene una extensión a una estructura $\mathfrak{B}$ de cualquier cardinalidad superior, tal que $\mathfrak{A}$ y $\mathfrak{B}$ son elementalmente equivalentes, excepto para la igualdad. No hay nada profundo acerca de esto, hasta que se agrega la igualdad.

23. Sean $\mathfrak{A}$ una estructura y g una función uno a uno con dom $g = |\mathfrak{A}|$. Muestre que hay una única estructura $\mathfrak{B}$ tal que g es un isomorfismo de $\mathfrak{A}$ sobre $\mathfrak{B}$.

24. Sea h una inmersión isomorfa de $\mathfrak{A}$ en $\mathfrak{B}$. Muestre que hay una estructura $\mathfrak{C}$ isomorfa a $\mathfrak{B}$ tal que $\mathfrak{A}$ es una subestructura de $\mathfrak{C}$. *Sugerencia:* Sea g una función uno a uno con dominio $|\mathfrak{B}|$ tal que $g(h(a)) = a$ para $a \in |\mathfrak{A}|$. Forme $\mathfrak{C}$ de manera tal que g sea un isomorfismo de $\mathfrak{B}$ sobre $\mathfrak{C}$.

    Comentario: No debería parecer sorprendente el resultado planteado en este ejercicio. Por el contrario, es una de esas afirmaciones que resultan obvias sólo hasta que tienen que probarse. Dice que si podemos hacer una inmersión isomorfa de $\mathfrak{A}$ en $\mathfrak{B}$, entonces para todos los propósitos prácticos podemos pretender que $\mathfrak{A}$ es una subestructura de $\mathfrak{B}$.

25. Considere una estructura fija $\mathfrak{A}$. Expanda el lenguaje añadiendo un nuevo símbolo de constante c_a para cada $a \in |\mathfrak{A}|$. Sea $\mathfrak{A}^+$ la estructura para este lenguaje expandido que concuerda con $\mathfrak{A}$ en los parámetros originales y que asigna a c_a el punto a. Se dice que una relación R sobre $|\mathfrak{A}|$ es ***definible a partir de puntos*** en $\mathfrak{A}$ sii R es definible en $\mathfrak{A}^+$. (Esto difiere de la definibilidad ordinaria sólo en que ahora tenemos parámetros en el lenguaje para los elementos de $|\mathfrak{A}|$. Sea $\mathfrak{R} = (\mathbb{R}; <, +, \cdot)$.

    (a) Muestre que si A es un subconjunto de $\mathbb{R}$ que consiste en la unión de una cantidad finita de intervalos, entonces A es definible a partir de puntos en $\mathfrak{R}$ (véase el ejercicio 12).

    (b) Suponga que $\mathfrak{A} \equiv \mathfrak{R}$. Muestre que cualquier subconjunto de $|\mathfrak{A}|$ que sea no vacío, acotado (con el orden $<^{\mathfrak{A}}$), y definible a partir de puntos en $\mathfrak{A}$ tiene una mínima cota superior en $|\mathfrak{A}|$.

    Digresión: Frecuentemente, cuando la gente habla de definibilidad dentro de una estructura, éste es el concepto al que se refieren. La frase más estándar es "definible a partir de parámetros"; aquí se usa "puntos", porque la palabra "parámetro" se está empleando en este capítulo en un sentido diferente.

El campo ordenado real puede ser caracterizado salvo isomorfismo al decir que es un campo ordenado completo. (Esto debería incluirse en todo curso de análisis.) Pero la completud (es decir, que los conjuntos acotados no vacíos tengan mínimas cotas superiores) no es una propiedad de primer orden. Véase el ejemplo 4 de la sección 1 del capítulo IV para su formulación en segundo orden. La "imagen" de completud en primer orden está dada por el esquema obtenido de esa afirmación de segundo orden, al sustituir X por una fórmula de primer orden φ. El esquema resultante (es decir, el conjunto de enunciados que obtenemos al permitir que la fórmula φ varíe y al tomar la cerradura universal) dice que la propiedad de mínima cota superior se cumple para los conjuntos que son definibles a partir de puntos. Los campos ordenados que satisfacen esos enunciados se llaman "campos ordenados real cerrados".

Lo sorprendente es que dichos campos no fueron inventados por los lógicos. Fueron estudiados con anterioridad por los algebristas y uno puede leer acerca de ellos en el volumen I del libro *Modern Algebra* de van der Waerden. Por supuesto, él utiliza una caracterización de dichos campos en la que no interviene la lógica.

Lo que Tarski mostró es que cualquier campo ordenado real cerrado es elementalmente equivalente al campo de los números reales. De esto se sigue que la teoría de campos ordenados real cerrados es decidible.

26. (a) Considere una estructura fija $\mathfrak{A}$ y defina su *tipo elemental* como la clase de estructuras elementalmente equivalentes a $\mathfrak{A}$. Muestre que esta clase es EC_Δ. *Sugerencia*: Muestre que es Mod Th $\mathfrak{A}$.

    (b) Llamemos a una clase $\mathcal{K}$ de estructuras *elementalmente cerrada* o ECL, si siempre que una estructura pertenece a $\mathcal{K}$, entonces todas las estructuras elementalmente equivalentes a ella también pertenecen a $\mathcal{K}$. Muestre que cualquier clase así es una unión de clases EC_Δ. (Se dice que cuando una clase es unión de

clases EC_Δ, es una clase $EC_{\Delta\Sigma}$; esta notación proviene de la topología.)

(c) De forma inversa, muestre que cualquier clase que sea una unión de clases EC_Δ es elementalmente cerrada.

27. Supongamos que los parámetros del lenguaje son $\forall$ y un símbolo de predicado P de dos argumentos. Haga una lista con todas las estructuras no isomorfas de tamaño 2. Esto es, dé una lista de estructuras (en donde el universo de cada una de ellas tenga tamaño 2) tal que cualquier estructura de tamaño 2 resulte isomorfa exactamente a una estructura de la lista.

28. Para cada uno de los siguientes pares de estructuras, muestre que no son elementalmente equivalentes, formulando un enunciado que sea verdadero en una y falso en la otra. (Aquí el lenguaje contiene $\forall$ y un símbolo de función de dos argumentos $\circ$.)

(a) $(\mathbb{R}; \times)$ y $(\mathbb{R}^*; \times^*)$, donde $\times$ es la operación de multiplicación usual sobre los números reales, $\mathbb{R}^*$ es el conjunto de reales diferentes de cero, y $\times^*$ es $\times$ restringida a los reales diferentes de cero.

(b) $(\mathbb{N}; +)$ y $(\mathbb{P}; +^*)$, donde $\mathbb{P}$ es el conjunto de los enteros positivos, y $+^*$ es la operación de suma usual restringida a $\mathbb{P}$.

(c) Mejor aún, para cada una de las cuatro estructuras de las partes (a) y (b), formule un enunciado verdadero en esa estructura y falso en las otras tres.

3. *Un algoritmo de análisis*[3]

Al igual que en la lógica de enunciados, necesitamos saber que podemos descomponer las fórmulas (y los términos) de una manera única para descubrir cómo están construidos. La unicidad es necesaria para justificar nuestras definiciones por recursión, como la definición de satisfacción que apareció en la sección precedente.

[3] El lector que esté dispuesto a aceptar el significado de nuestras muchas definiciones obtenidas por recursión puede prescindir de esta sección.

Para los términos utilizamos la notación polaca; para las fórmulas nos apoyamos en los paréntesis. Por lo tanto, primero consideramos un procedimiento de descomposición para los términos, mostrando la unicidad de la lectura, y posteriormente extendemos los métodos para hacerlo con las fórmulas.

Recordemos que los términos se construyen a partir de símbolos de constante y de variable, con operaciones correspondientes a los símbolos de función. Primero definimos una función K en los símbolos involucrados, de tal manera que para un símbolo s, $K(s) = 1 - n$, donde n es el número de términos que deben seguir a s para obtener un término:

$K(x) = 1-0 = 1$	para una variable x;
$K(c) = 1-0 = 1$	para un símbolo de constante c;
$K(f) = 1-n$	para un símbolo de función f de n argumentos.

Luego extendemos K al conjunto de expresiones que usan estos símbolos definiendo

$$K(s_1 s_2 \cdots s_n) = K(s_1) + K(s_2) + \cdots + K(s_n).$$

Ya que ningún símbolo es una sucesión finita de otros, esta definición no es ambigua.

Lema 23A Para cualquier término t, $K(t) = 1$.

Demostración Usamos inducción sobre t. El paso inductivo para un símbolo de función f de n argumentos es

$$K(f t_1 \cdots t_n) = (1 - n) + \underbrace{(1 + \cdots + 1)}_{n \text{ veces}} = 1.$$

⊣

De hecho, K fue escogida para ser la función de unicidad en estos símbolos para los cuales se cumple el lema 23A. De este lema se sigue que si ε es una concatenación de m términos, entonces $K(\varepsilon) = m$.

Con segmento *terminal* de una cadena $\langle s_1, \cdots, s_n \rangle$ de símbolos queremos decir una sucesión de la forma $\langle s_k, s_{k+1}, \cdots, s_n \rangle$, donde $1 \leq k \leq n$.

Lema 23B Cualquier segmento terminal de un término es una concatenación de uno o más términos.

Demostración Usamos inducción sobre el término. Para un término de un solo símbolo (es decir, un símbolo de constante o de variable) la conclusión se sigue de forma trivial. Para un término $f\, t_1 \cdots t_n$, cualquier segmento terminal (distinto del término mismo) deberá ser igual a

$$t'_k\, t_{k+1} \cdots t_n,$$

donde $k \leq n$ y t'_k es un segmento terminal de t_k. Por la hipótesis inductiva, t'_k es una concatenación de, digamos, m términos, donde $m \geq 1$. Así que en total tenemos $m + (n - k)$ términos. ⊣

Corolario 23C Ningún segmento inicial propio de un término es un término. Si t_1 es el segmento inicial propio de un término t, entonces $K(t_1) < 1$.

Demostración Supongamos que un término t se divide en un segmento inicial propio t_1 y un segmento terminal t_2. Entonces, $1 = K(t) = K(t_1) + K(t_2)$, y por el Lema 23B, $K(t_2) \geq 1$. De aquí que $K(t_1) < 1$ y t_1 no puede ser un término. ⊣

Análisis de términos

Queremos un algoritmo que, dada una expresión, determine si esa expresión es o no un término permitido y, en caso de serlo, construya el árbol de unicidad que muestre cómo se construye el término.

Supongamos que se nos da una expresión. Construiremos un árbol situando la expresión dada en la parte superior (es decir, la raíz). Inicialmente, es el único vértice en el árbol, pero a medida que el procedimiento avance, el árbol crecerá hacia abajo.

El algoritmo se compone de los dos pasos siguientes:

1. Si cada vértice minimal (en la parte inferior) tiene un único símbolo (que deberá* ser un símbolo de constante o de

variable), entonces el procedimiento termina. (La expresión dada es de hecho un término, y habremos construido su árbol.) De otra manera, seleccione un vértice minimal que tenga una expresión con dos o más símbolos. Examinamos esa expresión.

2. El primer símbolo deberá* ser un símbolo de función de n argumentos, digamos f, donde $n > 0$. Extendemos el árbol hacia abajo creando n nuevos vértices debajo del que ya tenemos. Revise la expresión después de f, hasta que alcance la primera cadena t (de variables, de símbolos de constante y de símbolos de función) con $K(t) = 1$.† Entonces t es la expresión que va al nuevo vértice sin etiqueta de la extrema izquierda. Repita con el resto de la expresión, hasta que se etiqueten todos los n nuevos vértices y se haya agotado la expresión.† Regrese al paso 1.

Al igual que en la sección 3 del capítulo I, el punto crucial es que el árbol no se podría haber hecho de forma diferente. En el paso 2, seleccionamos la primera cadena t que encontramos con $K(t) = 1$. No podíamos usar menos que t (debido a que necesitábamos que $K(t) = 1$ de acuerdo con el lema 23A). No podíamos usar más que t (debido a que una cadena más larga tendría el segmento inicial propio t con $K(t) = 1$, en contradicción con el corolario 23C). Elegir t era la única opción posible.

Cuando se detiene el logaritmo, lo que ha sucedido es que o bien se rechazó la expresión dada por no ser un término, o bien se construyó el único árbol que demuestra que la expresión dada es un árbol permitido.

Podemos reformular la unicidad, en la terminología de la sección 4 del capítulo 1, como sigue:

Teorema de unicidad de la lectura para términos El conjunto de términos se genera libremente a partir del conjunto de variables y de símbolos de constante mediante las operaciones $\mathcal{F}_f$.

*Si no, entonces la expresión presente no es un término. Rechazamos la expresión dada por no ser un término y nos detenemos.

†Si se alcanza el final de la expresión antes de encontrar tal t, entonces la expresión en cuestión no es un término. Rechazamos la expresión dada por no ser un término y nos detenemos.

Demostración Primero, resulta claro que si $f \neq g$, entonces ran $\mathcal{F}_f$ es disjunto de ran $\mathcal{F}_g$; esto requiere revisar únicamente el primer símbolo. Además, ambos rangos son disjuntos del conjunto de variables y símbolos de constante. Sólo resta mostrar que $\mathcal{F}_f$, cuando se restringe a los términos, es uno a uno. Supongamos que, para una f de dos argumentos, tenemos

$$f t_1 t_2 = f t_3 t_4.$$

Al eliminar el primer símbolo nos quedamos sólo con

$$t_1 t_2 = t_3 t_4.$$

Si $t_1 \neq t_3$, entonces uno sería un segmento inicial propio del otro, lo cual es imposible para los términos por el corolario 23C. Así que $t_1 = t_3$, y nos quedamos con $t_2 = t_4$. ⊣

Análisis de fórmulas

Para extender este razonamiento a las fórmulas, ahora definimos K para los otros símbolos:

$$K(() = -1;$$
$$K()) = 1;$$
$$K(\forall) = -1;$$
$$K(\neg) = 0;$$
$$K(\rightarrow) = -1;$$
$K(P) = 1 - n$ para un símbolo de predicado P de n argumentos;
$$K(=) = -1.$$

La idea que se encuentra detrás de la definición es, de nuevo, que $K(s)$ debería ser $1 - n$, donde n es el número de objetos (paréntesis derechos, términos o fórmulas) requeridos para ir después de s. Como se suele hacer, extendemos K al conjunto de todas las expresiones:

$$K(s_1 \cdots s_n) = K(s_1) + \cdots + K(s_n).$$

Lema 23D Para cualquier fórmula α, $K(\alpha) = 1$.

Demostración Otra inducción directa. ⊣

Lema 23E Para cualquier segmento inicial propio α' de una fórmula α, $K(\alpha') < 1$.

Demostración Use inducción sobre α. Los detalles se dejan para el ejercicio 1. ⊣

Corolario 23F Ningún segmento inicial propio de una fórmula es una fórmula.

Provistos de esta información, podemos proceder como en la sección 3 del capítulo I. En lugar de símbolos de enunciado en los vértices minimales, ahora tenemos fórmulas atómicas (las cuales se distinguen por tener primero un símbolo de predicado de n argumentos, seguido de n términos).

Una fórmula que no sea atómica deberá comenzar con $\forall v_i$ o con (. En el primer caso tenemos un nuevo vértice; en el segundo caso necesitamos examinar el siguiente símbolo para ver si es $\neg$. Si no lo es, entonces podemos contar los paréntesis o usar la función K —ambos métodos funcionan— para encontrar la división correcta.

De nuevo, la unicidad puede expresarse en la terminología de la sección 4 del capítulo 1 como sigue:

Teorema de unicidad de la lectura para fórmulas El conjunto de fórmulas se genera libremente a partir del conjunto de fórmulas atómicas mediante las operaciones $\mathcal{E}_\neg$, $\mathcal{E}_\rightarrow$ y Q_i ($i = 1, 2, \ldots$).

Demostración Las operaciones unarias $\mathcal{E}_\neg$ y Q_i son obviamente uno a uno. Al igual que en la sección 4 del capítulo 1, podemos mostrar que la restricción de $\mathcal{E}_\rightarrow$ a las fórmulas es uno a uno.

La parte del teorema de que las operaciones son ajenas es consecuencia de las siguientes observaciones *ad hoc*:

1. ran $\mathcal{E}_\neg$, ran Q_i, ran Q_j, y el conjunto de fórmulas atómicas son ajenos dos a dos, para $i \neq j$. (Sólo observe los dos primeros símbolos.)

2. ran $\mathcal{E}_\rightarrow$, ran Q_i, ran Q_j, y el conjunto de fórmulas atómicas son igualmente ajenos dos a dos, para $i \neq j$.

3. Para una fórmula β, $(\neg\alpha) \neq (\beta \rightarrow \gamma)$ debido a que ninguna fórmula empieza con $\neg$. De aquí que ran $\mathcal{E}_\neg$ sea disjunto del rango de la restricción de $\mathcal{E}_\rightarrow$ a las fórmulas. ⊣

Ejercicios

1. Muestre que, para un segmento inicial propio α' de una fórmula α, tenemos que $K(\alpha') < 1$.

2. Sea ε una expresión compuesta de variables, símbolos de constante y símbolos de función. Muestre que ε es un término sii $K(\varepsilon) = 1$ y para todo segmento terminal ε' de ε tenemos $K(\varepsilon') > 0$. *Sugerencia*: Pruebe el resultado más fuerte, que si $K(\varepsilon') > 0$ para todo segmento terminal ε' de ε, entonces ε es una concatenación de $K(\varepsilon)$ términos. (Este algoritmo se debe a Jáskowski.)

4. *Un cálculo deductivo*

Suponga que $\Sigma \models \tau$. ¿Qué métodos de demostración se requerirían para demostrar ese hecho?; ¿hay necesariamente una demostración?

Tales preguntas conducen inmediatamente a examinar qué constituye una demostración. Una demostración es un argumento que se da a otra persona y que la convence completamente de la correctud de nuestra aseveración (en este caso, de que $\Sigma \models \tau$).

Entonces una demostración deberá tener longitud finita, ya que no se le puede dar la totalidad de un objeto infinito a otra persona. Si el conjunto Σ de hipótesis es infinito, no pueden usarse todas. Pero el teorema de compacidad para la lógica de primer orden (que probaremos en la sección 5 de este capítulo usando el cálculo deductivo de esta sección) asegurará la existencia de un Σ_0 finito, $\Sigma_0 \subseteq \Sigma$, tal que $\Sigma_0 \models \tau$.

Otra característica esencial de una demostración (además de ser finita en su longitud) es que debe ser posible que alguien

más (si esa persona ha de quedar convencida de ella) verifique la demostración para asegurarse de que no contiene falacias. Esta verificación deberá ser efectiva; deberá ser del tipo de procesos que puede realizarse sin necesidad de intuiciones brillantes por parte del verificador. En particular, el conjunto de demostraciones a partir del conjunto vacío de hipótesis (es decir, demostraciones de que $\models \tau$) deberá ser decidible. Esto implica que el conjunto de fórmulas demostrables sin hipótesis tiene que ser efectivamente numerable, ya que en principio uno podría enumerar los enunciados demostrables generando todas las cadenas de símbolos y separando las demostraciones de las que no son demostraciones. Cuando se descubre una demostración, su última línea se ingresa en la lista de salida. (Este asunto se examinará con mayor profundidad al final de la sección 5 de este capítulo.) Pero de nuevo hay aquí un teorema (el teorema de numerabilidad, probado en la sección 5 de este capítulo) que dice que en condiciones razonables, las fórmulas válidas, es decir, el conjunto de fórmulas válidas, es de hecho efectivamente numerable.

Por consiguiente, el teorema de compacidad y el teorema de numerabilidad son condiciones necesarias para llegar a demostraciones satisfactorias de la implicación lógica. A la inversa, afirmamos que estos dos teoremas son suficientes para que existan demostraciones (de cierto tipo). Supongamos que $\Sigma \models \tau$. Por el teorema de compacidad, entonces, hay un conjunto finito $\{\sigma_0, \ldots, \sigma_n\} \subseteq \Sigma$ que implica lógicamente a τ. Entonces, $\sigma_0 \to \cdots \to \sigma_n \to \tau$ es válida (ejercicio 1 de la sección 2 de este capítulo). Así que para demostrar de manera concluyente que $\Sigma \models \tau$ sólo tenemos que ejecutar un número finito de pasos en la numeración de las fórmulas válidas hasta que aparezca $\sigma_0 \to \cdots \to \sigma_n \to \tau$, y después verificar que cada $\sigma_i \in \Sigma$. (Esto deberá compararse con el complejo procedimiento sugerido por la definición original de implicación lógica, y que discutimos en la sección 2 de este capítulo.) El registro del procedimiento de enumeración que produjo $\sigma_0 \to \cdots \to \sigma_n \to \tau$ puede entonces considerarse como una *demostración* de que $\Sigma \models \tau$. Como demostración, deberá ser aceptable para cualquiera que acepte la correctud del procedimiento para enumerar las fórmulas válidas.

En contra de la precedente discusión general (y ligeramente vaga), el contenido de esta sección puede esbozarse de la siguiente manera: introduciremos demostraciones formales, pero las llamaremos *deducciones*, para evitar que sean confundidas con nuestras demostraciones en español. Éstas reflejarán (en nuestro modelo de pensamiento deductivo) las demostraciones hechas por el matemático activo para convencer a sus colegas de ciertas verdades. Después, en la sección 5 de este capítulo, mostraremos que siempre que $\Sigma \models \tau$, hay una deducción de τ a partir de Σ (y sólo entonces). Esto, como se sugiere en la discusión anterior, dará como resultado las demostraciones del teorema de compacidad y del teorema de numerabilidad. Y durante el proceso podremos observar qué métodos de deducción son adecuados para demostrar que un determinado enunciado de hecho está implicado lógicamente por otros enunciados. En otras palabras, nuestra meta es generar un concepto de deducción matemáticamente preciso, que sea adecuado y correcto en el contexto de la lógica de primer orden.

Deducciones formales

En breve, elegiremos un conjunto Λ infinito de fórmulas que se llamarán axiomas lógicos. Asimismo tendremos una regla de inferencia que nos permitirá obtener una nueva formula a partir de algunas otras fórmulas. Luego, para un conjunto Γ de fórmulas, los *teoremas* de Γ serán las fórmulas que pueden obtenerse de $\Gamma \cup \Lambda$ usando la regla de inferencia (un número finito de veces). Si φ es un teorema de Γ (que se escribe: $\Gamma \vdash \varphi$), entonces, una sucesión de fórmulas que describa (como se explica más adelante) cómo se obtuvo φ a partir de $\Gamma \cup \Lambda$ con la regla de inferencia se denominará una deducción de φ a partir de Γ.

La elección de Λ y la elección de la regla (o reglas) de inferencia distan de ser únicas. En esta sección presentamos un cálculo deductivo para la lógica de primer orden, elegido de entre todos los cálculos posibles. (Por ejemplo, podemos tener $\Lambda = \emptyset$ usando muchas reglas de inferencia. Adoptaremos el extremo opuesto; nuestro conjunto Λ será infinito pero sólo tendremos una regla de inferencia.)

Nuestra única regla de inferencia se conoce tradicionalmente como *modus ponens*. Se suele expresar así: a partir de las fórmulas α y $\alpha \to \beta$ podemos inferir β:

$$\frac{\alpha, \ \alpha \to \beta}{\beta}.$$

Entonces los teoremas del conjunto Γ son las fórmulas que se pueden obtener a partir de $\Gamma \cup \Lambda$ usando modus ponens un número finito de veces.

Definición Una *deducción de φ a partir de* Γ es una sucesión finita $\langle \alpha_0, \ldots, \alpha_n \rangle$ de fórmulas tal que α_n es φ y para cada $k \leq n$, o bien

(a) α_k está en $\Gamma \cup \Lambda$, o bien,

(b) α_k se obtiene mediante modus ponens a partir de dos fórmulas anteriores de la sucesión; esto es, para algunos i y j menores que k, α_j es $\alpha_i \to \alpha_k$.

Si tal deducción existe, decimos que φ es *deducible* a partir de Γ, o que φ es un *teorema* de Γ, y lo escribimos $\Gamma \vdash \varphi$.

Hay otro punto de vista que resulta útil aquí: una deducción de φ a partir de Γ puede verse como una *sucesión de construcción*, que muestra cómo se puede obtener φ a partir del conjunto $\Gamma \cup \Lambda$ al aplicar modus ponens cero o más veces. (Vacilamos al decir que φ se "construye" a partir de $\Gamma \cup \Lambda$, pues, a diferencia de las operaciones de construcción de fórmulas que generan fórmulas más largas a partir de otras más cortas, el modus ponens puede generar fórmulas más cortas a partir de otras más largas.) Esto es, el conjunto de teoremas de Γ es exactamente el conjunto de fórmulas que se pueden obtener del conjunto "base" $\Gamma \cup \Lambda$ mediante la aplicación de modus ponens.

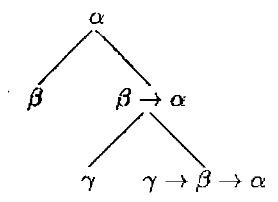
Esta situación difiere en dos sentidos, uno irrelevante y otro importante, de la situación que se discutió en la sección 4 del capítulo I. La diferencia irrelevante es que obtenemos el conjunto de teoremas al cerrar bajo la operación "parcialmente definida" de modus ponens, cuyo dominio únicamente se compone de pares de fórmulas de la forma $\langle \alpha, \ \alpha \to \beta \rangle$ (en contraste con las operaciones "totalmente definidas" de construcción de

fórmulas). La diferencia más importante es que el conjunto de teoremas *no* se genera libremente a partir de $\Gamma \cup \Lambda$ mediante modus ponens. Esto refleja el hecho de que un teorema nunca tiene una deducción *única*. En las secciones 3 del capítulo 1 y 3 de este capítulo, nos interesaba mostrar que para cualquier fórmula φ, había un árbol único (que podíamos calcular efectivamente) mostrando cómo se construyó φ usando operaciones de construcción de fórmulas. Ahora bien, el árbol no es único en modo alguno, y calcular dicho árbol es ahora un asunto muy diferente.

Sin embargo, este punto de vista sí genera el siguiente principio de inducción. Decimos que un conjunto S de fórmulas está *cerrado* bajo modus ponens si siempre que ambos $\alpha \in S$ y $(\alpha \to \beta) \in S$ entonces también $\beta \in S$.

Principio de inducción Supongamos que S es un conjunto de fórmulas que incluye $\Gamma \cup \Lambda$ y que está cerrado bajo modus ponens. Entonces S contiene todos los teoremas de Γ.

Por ejemplo, si las fórmulas β, γ y $\gamma \to \beta \to \alpha$ se encuentran todas en $\Gamma \cup \Lambda$, entonces $\Gamma \vdash \alpha$, como es evidente por el árbol siguiente, que muestra cómo se obtuvo α. Aunque resulta tentador (y de alguna manera más elegante) definir una deducción como tal árbol, será más simple considerar las deducciones como las sucesiones lineales que se obtienen al aplastar esos árboles en líneas rectas.



Ahora finalmente damos el conjunto Λ de axiomas lógicos. Éstos están dispuestos en seis grupos. Diremos que una fórmula φ es una *generalización* de ψ sii para alguna $n \geq 0$ y variables $x_1, \ldots, x_n$,

$$\varphi = \forall x_1 \cdots \forall x_n \, \psi.$$

Incluimos el caso $n = 0$; cualquier fórmula es una generalización de sí misma. Entonces, los axiomas lógicos son todos generalizaciones de fórmulas de las formas siguientes, donde x y y son variables y α y β son fórmulas:

1. Tautologías;
2. $\forall x\, \alpha \rightarrow \alpha_t^x$, donde t se puede sustituir por x en α;
3. $\forall x(\alpha \rightarrow \beta) \rightarrow (\forall x\, \alpha \rightarrow \forall x\, \beta)$;
4. $\alpha \rightarrow \forall x\, \alpha$, donde x no ocurre libre en α.

Y si el lenguaje incluye igualdad, entonces agregamos

5. $x = x$;
6. $x = y \rightarrow (\alpha \rightarrow \alpha')$, donde α es atómica y α' se obtiene de α al reemplazar x por y en cero o más lugares (aunque no necesariamente en todos).

En su mayor parte, los grupos 3–6 se explican por sí mismos; veremos varios ejemplos más adelante. Los grupos 1 y 2 requieren explicación. No obstante, primero debemos admitir que tal vez la lista anterior de axiomas lógicos no parezca muy natural. Más adelante se podrá ver dónde se originó cada uno de los seis grupos.

Sustitución

En el grupo 2 de axiomas encontramos

$$\forall x\, \alpha \rightarrow \alpha_t^x.$$

Aquí, α_t^x es la expresión que se obtiene de la fórmula α al reemplazar la variable x, dondequiera que ocurra libre en α, por el término t. Este concepto también se puede definir (y para nosotros es su definición oficial) por recursión:

1. Para α atómica, α_t^x es la expresión que se obtiene de α al reemplazar la variable x por t. (Esto se elaborará en el ejercicio 1. Nótese que α_t^x es también una fórmula.)
2. $(\neg\alpha)_t^x = (\neg\alpha_t^x)$.

3. $(\alpha \to \beta)^x_t = (\alpha^x_t \to \beta^x_t)$.

4. $(\forall y\, \alpha)^x_t = \begin{cases} \forall y\, \alpha & \text{si } x = y, \\ \forall y\, (\alpha^x_t) & \text{si } x \neq y. \end{cases}$

EJEMPLOS

1. $\varphi^x_x = \varphi$.
2. $(Qx \to \forall x\, Px)^x_y = (Qy \to \forall x\, Px)$.
3. Si α es $\neg \forall y\; x = y$, entonces $\forall x\, \alpha \to \alpha^x_z$ es

$$\forall x \neg \forall y\; x = y \to \neg \forall y\; z = y.$$

4. Para α como en 3, $\forall x\, \alpha \to \alpha^x_y$ es

$$\forall x \neg \forall y\; x = y \to \neg \forall y\; y = y.$$

El último de los ejemplos ilustra el peligro del que debemos cuidarnos. En su conjunto, $\forall x\, \alpha \to \alpha^x_t$ aparenta ser un axioma suficientemente plausible. ("Si α es verdadero para todos, entonces debería ser verdadero para t.") Pero en el ejemplo 4 tenemos un enunciado de la forma $\forall x\, \alpha \to \alpha^x_t$, que casi siempre es falso. El antecedente, $\forall x\, \neg \forall y\; x = y$, es verdadero en cualquier estructura cuyo universo contenga dos o más elementos. Pero el consecuente $\neg \forall y\; y = y$ es falso en cualquier estructura. Así que algo anda mal.

El problema es que cuando se sustituyó y por x, fue "capturada" inmediatamente por el cuantificador $\forall y$. Debemos imponer una restricción al grupo 2 de axiomas que prevenga este tipo de captura del cuantificador. De manera informal podemos decir que un término t *no* es sustituible por x en α si hay alguna variable y en t que esté capturada por el cuantificador $\forall y$ en α^x_t. La verdadera definición se dará más adelante por recursión. (Ya que este concepto se usará posteriormente en demostraciones por inducción, una definición recursiva es de hecho la forma que más se puede utilizar.)

Sean x una variable y t un término. Definimos la frase "t es sustituible por x en α" de la manera siguiente:

1. Para α atómica, t siempre es sustituible por x en α. (No hay cuantificadores en α, así que no puede ocurrir ninguna captura.)

2. t es sustituible por x en $(\neg \alpha)$ sii es sustituible por x en α. t es sustituible por x en $(\alpha \rightarrow \beta)$ sii es sustituible por x tanto en α como en β.

3. t es sustituible por x en $\forall y\ \alpha$ sii o bien

   (a) x no ocurre libre en $\forall y\ \alpha$, o bien

   (b) y no ocurre en t y t es sustituible por x en α.

(Lo importante es asegurarse de que nada en t sea capturado por el prefijo $\forall y$ y que nada haya fallado antes dentro de α.)

Por ejemplo, x siempre es sustituible por sí misma en cualquier fórmula. Si t no tiene variables que ocurran en α, entonces t es sustituible por x en α.

Se advierte al lector que no se confunda con la elección de las palabras. Aun cuando t no sea sustituible por x en α, todavía se puede obtener α_t^x de α al reemplazar x por t siempre que la primera ocurra libremente. Por lo tanto, al formar α_t^x, realizamos la sustitución indicada, aun cuando una persona prudente piense que es incorrecto hacerlo.

El grupo 2 de axiomas se compone de todas las generalizaciones de las fórmulas de la forma

$$\forall x\, \alpha \rightarrow \alpha_t^x,$$

donde el término t es sustituible por la variable x en la fórmula α. Por ejemplo,

$$\forall v_3(\forall v_1(A\, v_1 \rightarrow \forall v_2 A\, v_2) \rightarrow (A\, v_2 \rightarrow \forall v_2 A\, v_2))$$

se encuentra en el grupo 2 de axiomas. Aquí, x es v_1, α es $A\, v_1 \rightarrow \forall v_2 A\, v_2$, y t es v_2. Por otra parte,

$$\forall v_1\, \forall v_2\ B\, v_1\, v_2 \rightarrow \forall v_2 B\, v_2\, v_2$$

no se encuentra en el grupo 2 de axiomas, ya que v_2 no es sustituible por v_1 en $\forall v_2 B\, v_1\, v_2$.

Tautologías

El grupo 1 de axiomas comprende las generalizaciones de las fórmulas que llamaremos *tautologías*. Éstas son las fórmulas que se pueden obtener a partir de tautologías de la lógica de enunciados (que tienen únicamente los símbolos de conectivo $\neg$ y $\rightarrow$) al reemplazar cada símbolo de enunciado por una fórmula del lenguaje de primer orden. Por ejemplo,

$$\forall x[(\forall y \neg Py \rightarrow \neg Px) \rightarrow (Px \rightarrow \neg \forall y \neg Py)]$$

pertenece al grupo 1 de axiomas. Es una generalización de la fórmula en corchetes, la cual se obtiene de una tautología contraposición

$$(\mathbf{A} \rightarrow \neg\mathbf{B}) \rightarrow (\mathbf{B} \rightarrow \neg\mathbf{A})$$

al reemplazar **A** por $\forall y \neg Py$ y **B** por Px.

Existe otra manera más directa de examinar el grupo 1 de axiomas. Dividimos las fórmulas en dos grupos:

1. Las fórmulas *primas* son las fórmulas atómicas y aquellas de la forma $\forall x\, \alpha$.

2. Las fórmulas no primas son todas las demás; es decir, aquellas de la forma $\neg\alpha$ o $\alpha \rightarrow \beta$.

Por lo tanto, cualquier fórmula se construye a partir de fórmulas primas mediante las operaciones $\mathcal{E}_{\neg}$ y $\mathcal{E}_{\rightarrow}$. Ahora regresemos a la lógica de enunciados, pero tomemos como símbolos de enunciado las fórmulas primas de nuestro lenguaje de primer orden. Entonces, cualquier tautología de la lógica de enunciados (que usa únicamente los símbolos de conectivo $\neg$ y $\rightarrow$) se encuentra en el grupo 1 de axiomas. En este caso no hay necesidad de *reemplazar* los símbolos de enunciado por fórmulas de primer orden; ya *son* fórmulas de primer orden. A la inversa, cualquier fórmula del grupo 1 de axiomas es una generalización de una tautología de la lógica de enunciados. (El ejercicio 8 de la sección 2 del capítulo I se usa para demostrar esto.)

EJEMPLO revisado.

$$(\forall y \neg Py \rightarrow \neg Px) \rightarrow (Px \rightarrow \neg \forall y \neg Py).$$

Éste tiene dos símbolos de enunciado (fórmulas primas), $\forall y \neg Py$ y Px. Así que su tabla de verdad tiene cuatro líneas:

$$
\begin{array}{llllllllll}
(\forall y \neg Py & \rightarrow & \neg & Px) & \rightarrow & (Px & \rightarrow & \neg & \forall y \neg Py) \\
V & F & F & V & V & V & F & F & V \\
V & V & V & F & V & F & V & F & V \\
F & V & F & V & V & V & V & V & F \\
F & V & V & F & V & F & V & V & F
\end{array}
$$

A partir de la tabla, podemos ver que efectivamente se trata de una tautología.

Por otro lado, ni $\forall x (Px \rightarrow Px)$ ni $\forall x\, Px \rightarrow Px$ son tautologías.

Un comentario: No hemos supuesto que nuestro lenguaje de primer orden tenga sólo una cantidad numerable de fórmulas. Así que utilizamos potencialmente una extensión del capítulo I para el caso de un conjunto no numerable de símbolos de enunciado.

Un segundo comentario: Tomar *todas* las tautologías como axiomas lógicos es un exceso. Podemos arreglárnoslas con mucho menos, a costa de extender las deducciones. Por una parte, las tautologías forman un buen conjunto decidible (la decidibilidad será importante para el teorema de numerabilidad de la sección 5 de este capítulo). Por otra parte, no se conoce ningún procedimiento *rápido* de decisión para las tautologías, como lo hicimos notar en la sección 7 del capítulo I. Una opción sería reducir el grupo 1 de axiomas y convertirlo en un conjunto de tautologías para las cuales sí conozcamos procedimientos rápidos de decisión (el término técnico es "decidible en tiempo polinomial"). Las otras tautologías podrán obtenerse luego a partir de éstas, por modus ponens.

Un tercer comentario: Ahora que las fórmulas de primer orden son también fórmulas de la lógica de enunciados, podemos aplicar a ellas conceptos de ambos capítulos 1 y II. Si Γ implica tautológicamente φ, entonces se sigue que Γ también implica lógicamente φ. (Véase el ejercicio 3.) Pero la inversa es falsa. Por ejemplo, $\forall x\, Px$ implica lógicamente Pc. Pero $\forall x\, Px$ *no* implica tautológicamente Pc, ya que $\forall x\ Px$ y Pc son dos símbolos de enunciado diferentes.

Teorema 24B $\Gamma \vdash \varphi$ sii $\Gamma \cup \Lambda$ implica tautológicamente φ.

Demostración ($\Rightarrow$): Esto depende del hecho obvio de que $\{\alpha, \alpha \to \beta\}$ implica tautológicamente β. Supongamos que tenemos una asignación de verdad v que satisface todos los elementos de $\Gamma \cup \Lambda$. Por inducción, podemos observar que v satisface cualquier teorema de Γ. El paso inductivo utiliza exactamente el hecho obvio mencionado anteriormente.

($\Leftarrow$): Supongamos que $\Gamma \cup \Lambda$ implica tautológicamente φ. Entonces, de acuerdo con el corolario del teorema de compacidad (para la lógica de enunciados), hay un subconjunto finito $\{\gamma_1, \ldots, \gamma_m, \lambda_1, \ldots, \lambda_n\}$ que implica tautológicamente φ. En consecuencia,

$$\gamma_1 \to \cdots \to \gamma_m \to \lambda_1 \to \cdots \to \lambda_n \to \varphi$$

es una tautología (véase el ejercicio 4 de la sección 2 del capítulo 1) y por lo tanto se encuentra en Λ. Al aplicar modus ponens $m + n$ veces a esta tautología y a $\{\gamma_1, \ldots, \gamma_m, \lambda_1, \ldots, \lambda_n\}$ obtenemos φ. ⊣

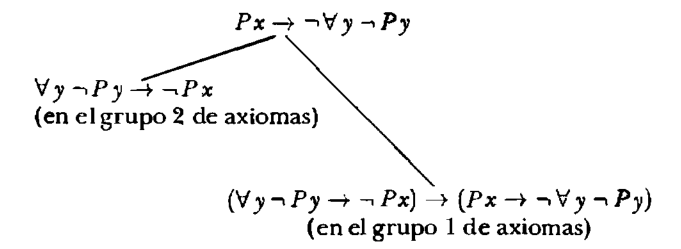
(La prueba anterior est relacionada con el ejercicio 7 de la sección 7 del capítulo I. Utiliza compacidad de enunciados para un lenguaje posiblemente no numerable.)

Deducciones y metateoremas

Ahora hemos completado la descripción del conjunto Λ de axiomas lógicos. El conjunto de teoremas de un conjunto Γ es el conjunto generado a partir de $\Gamma \cup \Lambda$ por modus ponens. Por ejemplo,

$$\vdash Px \to \exists y\, Py.$$

(Aquí, $\Gamma = \emptyset$; escribimos "$\vdash \alpha$" en lugar de "$\emptyset \vdash \alpha$".) La fórmula $Px \to \exists y\ Py$ se puede obtener aplicando modus ponens (una vez) a dos elementos de Λ, tal como se muestra en el siguiente árbol:



Al comprimir este árbol cn una sucesión lineal de tres elementos, obtenemos una deducción de $Px \to \exists y\, Py$ (a partir de $\emptyset$).

Como segundo ejemplo, podemos obtener una generalización de la fórmula del primer ejemplo:

$$\vdash \forall x (Px \to \exists y\, Py).$$

Lo anterior se observa en el siguiente árbol, que muestra la construcción de $\forall x (Px \to \exists y\, Py)$ a partir de Λ, por modus ponens:

$\forall x (Px \to \neg\forall y \neg Py)$

$\forall x(\forall y \neg Py \to \neg Px)$
(en el grupo 2 de axiomas)

$\forall x (\forall y \neg Py \to \neg Px) \to \forall x (Px \to \neg\forall y \neg Py)$

(un elemento del grupo 3 de axiomas)

$\forall x[(\forall y \neg Py \to \neg Px) \to (Px \to \neg\forall y \neg Py)]$
(en el grupo 1 de axiomas)

De nuevo podemos comprimir este árbol y convertirlo en una deducción.

En estos ejemplos parece que los árboles genealógicos salieron de la nada. Pero en breve desarrollaremos técnicas para

generar dichos árboles de una manera un tanto sistemática. Estas técnicas dependerán mucho del teorema de generalización y del teorema de la deducción que aparecen más adelante.

Nótese que usamos la palabra "teorema" en dos niveles diferentes. Decimos que α es un teorema de Γ si $\Gamma \vdash \alpha$. También hacemos muchas afirmaciones en español a cada una de las cuales la llamamos teorema, tal como la que aparece abajo. Parece poco probable que surja alguna confusión. Las afirmaciones en español podrían llamarse *metateoremas* para subrayar el hecho de que son resultados sobre deducciones y teoremas.

El teorema de generalización refleja nuestra idea intuitiva de que si podemos probar $__x__$ sin suponer nada en especial sobre x, entonces tenemos derecho a decir que "debido a que x era arbitrario, tenemos que $\forall x __x__$".

Teorema de generalización Si $\Gamma \vdash \varphi$ y x no ocurre libre en ninguna fórmula de Γ, entonces $\Gamma \vdash \forall x\, \varphi$.

Demostración Consideremos un conjunto Γ y una variable x no libre en Γ. Por inducción, mostraremos que para cualquier teorema φ de Γ, tenemos $\Gamma \vdash \forall x\, \varphi$. Para esto (por el principio de inducción) es suficiente mostrar que el conjunto

$$\{\varphi \mid \Gamma \vdash \forall x \varphi\}$$

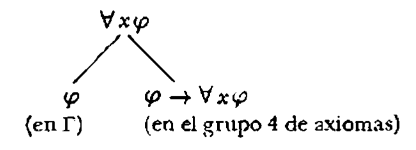
incluye $\Gamma \cup \Lambda$ y está cerrado bajo modus ponens. Nótese que x *puede* ocurrir libre en φ.

Caso 1: φ es un axioma lógico. Entonces $\forall x\, \varphi$ también es un axioma lógico. Y así $\Gamma \vdash \forall x\, \varphi$.

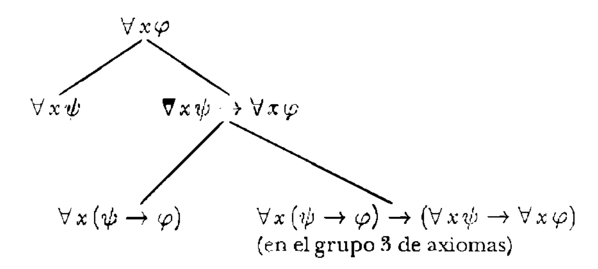
Caso 2: $\varphi \in \Gamma$. Entonces x no ocurre libre en φ. De aquí que

$$\varphi \to \forall x\, \varphi$$

está en el grupo 4 de axiomas. En consecuencia, $\Gamma \vdash \forall x \varphi$, como se evidencia mediante el árbol:



Caso 3: φ se obtiene por modus ponens de ψ y $\psi \to \varphi$. Entonces, por hipótesis inductiva tenemos $\Gamma \vdash \forall x\, \psi$ y $\Gamma \vdash \forall x\,(\psi \to \varphi)$. Ésta es la situación en la que justamente resulta útil el grupo 3 de axiomas. Que $\Gamma \vdash \forall x \varphi$ es evidente por el árbol:



Así que, por inducción, $\Gamma \vdash \forall x\, \varphi$ para cada teorema φ de Γ. ⊣

(Las únicas razones para tener los grupos de axiomas 3 y 4 se indican en la prueba anterior.)

La restricción de que x no ocurra libre en Γ es esencial. Por ejemplo, $Px \not\models \forall x\, Px$, y entonces, por el teorema de correctud que veremos en la sección 5 de este capítulo, $Px \nvdash \forall x\ Px$. Por otra parte, en general x ocurrirá libre en la fórmula φ. Por ejemplo, al principio de esta subsección mostramos primero que

$$\vdash (Px \to \exists y\, Py).$$

El segundo ejemplo ahí,

$$\vdash \forall x\,(Px \to \exists y\, Py),$$

se obtuvo del primer ejemplo, como en el caso 3 de la demostración anterior.

EJEMPLO $\forall x \forall y\, \alpha \vdash \forall y \forall x\, \alpha$.

La demostración del teorema de generalización realmente nos da un resultado más fuerte de lo que dice el enunciado. Muestra cómo, dada una deducción de φ a partir de Γ, podemos transformarla efectivamente para obtener una deducción de $\forall x\, \varphi$ a partir de Γ.

Lema 24C (Regla T) Si $\Gamma \vdash \alpha_1, \ldots, \Gamma \vdash \alpha_n$ y $\{\alpha_1, \ldots, \alpha_n\}$ implica tautológicamente β, entonces $\Gamma \vdash \beta$.

Demostración $\alpha_1 \to \cdots \to \alpha_n \to \beta$ es una tautología y, por tanto, un axioma lógico. Aplique modus ponens n veces. ⊣

Teorema de la deducción Si $\Gamma; \gamma \vdash \varphi$, entonces $\Gamma \vdash (\gamma \to \varphi)$.

(Está claro que el inverso también se cumple; de hecho, el inverso es esencialmente la regla modus ponens.)

Primera demostración

$\Gamma; \gamma \vdash \varphi$ sii $(\Gamma; \gamma) \cup \Lambda$ implica tautológicamente φ,
sii $\Gamma \cup \Lambda$ implica tautológicamente $(\gamma \to \varphi)$,
sii $\Gamma \vdash (\gamma \to \varphi)$.
⊣

Segunda demostración Esta demostración no usa el teorema de compacidad de la lógica de enunciados como lo hace la primera demostración. Muestra de una manera directa cómo transformar una deducción de φ a partir de $\Gamma;\gamma$ para obtener una deducción de $(\gamma \to \varphi)$ a partir de Γ. Por inducción, mostramos que para todo teorema φ de $\Gamma; \gamma$ la fórmula $(\gamma \to \varphi)$ es un teorema de Γ.

Caso 1: $\varphi = \gamma$. Entonces obviamente $\vdash (\gamma \to \varphi)$.

Caso 2: φ es un axioma lógico o un elemento de Γ. Entonces, $\Gamma \vdash \varphi$, y como φ implica tautológicamente $(\gamma \to \varphi)$, por la regla T tenemos $\Gamma \vdash (\gamma \to \varphi)$.

Caso 3: φ se obtiene de ψ y de $\psi \to \varphi$ por modus ponens. Por hipótesis inductiva, $\Gamma \vdash (\gamma \to \psi)$ y $\Gamma \vdash (\gamma \to (\psi \to \varphi))$. Y el conjunto $\{\gamma \to \psi, \gamma \to (\psi \to \varphi)\}$ implica tautológicamente $\gamma \to \varphi$. Por lo tanto, por la regla T, $\Gamma \vdash (\gamma \to \varphi)$.

Así, la conclusión se sigue por inducción para cualquier φ deducible de $\Gamma; \gamma$. ⊣

Corolario 24D (Contraposición) $\Gamma; \varphi \vdash \neg\psi$ sii $\Gamma; \psi \vdash \neg\varphi$.

Demostración

$\Gamma; \varphi \vdash \neg\psi \Rightarrow \Gamma \vdash \varphi \rightarrow \neg\psi$	por el teorema de la deducción,
$\Rightarrow \Gamma \vdash \psi \rightarrow \neg\varphi$	por la regla T,
$\Rightarrow \Gamma ; \psi \vdash \neg\varphi$	por modus ponens.

(En el segundo paso utilizamos el hecho de que $\varphi \rightarrow \neg\psi$ implica tautológicamente $\psi \rightarrow \neg\varphi$.) Por simetría, el inverso también se cumple. ⊣

Decimos que un conjunto de fórmulas es *inconsistente* sii para algún β, tanto β como $\neg\beta$ son teoremas del conjunto. (En este caso, cualquier fórmula α es un teorema del conjunto, ya que $\beta \rightarrow \neg\beta \rightarrow \alpha$ es una tautología.)

Corolario 24E (Reducción al absurdo) Si $\Gamma; \varphi$ es inconsistente, entonces $\Gamma \vdash \neg\varphi$.

Demostración Por el teorema de la deducción tenemos que $\Gamma \vdash (\varphi \rightarrow \beta)$ y $\Gamma \vdash (\varphi \rightarrow \neg\beta)$. Y $\{\varphi \rightarrow \beta, \varphi \rightarrow \neg\beta\}$ implica tautológicamente $\neg\varphi$. ⊣

EJEMPLO $\vdash \exists x \forall y\, \varphi \rightarrow \forall y \exists x\, \varphi$.

Trabajar hacia atrás da ciertas ventajas estratégicas.

Es suficiente mostrar que $\exists x \forall y\, \varphi \vdash \forall y \exists x\, \varphi$, por el teorema de la deducción.

Es suficiente mostrar que $\exists x\, \forall y\, \varphi \vdash \exists x\, \varphi$, por el teorema de generalización.

Es suficiente mostrar que $\neg\forall x \neg\forall y\, \varphi \vdash \neg\forall x \neg\varphi$, ya que es lo mismo que lo anterior.

Es suficiente mostrar que $\forall x\, \neg\varphi \vdash \forall x\, \neg\forall y\, \varphi$, por contraposición (y por la regla T).

Es suficiente mostrar que $\forall x \neg\varphi \vdash \neg\forall y\, \varphi$, por generalización.

Es suficiente mostrar que $\{\forall x\, \neg\varphi, \forall y\, \varphi\}$ es inconsistente, por reducción al absurdo.

Y esto es fácil:

1. $\forall x\, \neg\varphi \vdash \neg\varphi$, por el grupo 2 de axiomas y modus ponens.

2. $\forall y\ \varphi \vdash \varphi$ por la misma razón.

Las líneas 1 y 2 muestran que $\{\forall x\ \neg\varphi, \forall y\ \varphi\}$ es inconsistente.

Estrategia

Como lo indica el ejemplo anterior, los teoremas de generalización y de la deducción (y en menor medida los corolarios) serán muy útiles para mostrar que ciertas fórmulas son deducibles. Pero aún tenemos el asunto de la estrategia: para un Γ y un φ dados, ¿dónde deberíamos comenzar para poder demostrar que $\Gamma \vdash \varphi$? En principio se podría empezar enumerando todas las sucesiones finitas de fórmulas hasta encontrar una deducción de φ a partir de Γ. Aunque éste sería un procedimiento efectivo (para lenguajes razonables) para localizar una deducción si acaso existe alguna, es demasiado ineficiente si se tiene más que un interés teórico.

Una técnica consiste en abandonar la formalidad y dar en español una prueba de que la verdad de Γ implica la verdad de φ. Después se puede formalizar la prueba en español y realizar con ella una deducción formal. (En las páginas siguientes veremos técnicas para realizar tal formalización de una manera razonablemente natural.)

También hay métodos útiles que se basan únicamente en la forma sintáctica de φ. Supongamos entoces que φ es de hecho deducible a partir de Γ, pero que estamos buscando la prueba de este hecho. Hay varios casos:

1. Supongamos que φ es $(\psi \to \theta)$. Entonces será suficiente mostrar que $\Gamma; \psi \vdash \theta$ (y esto siempre será posible).

2. Supongamos que φ es $\forall x\ \psi$. Si x no ocurre libre en Γ, entonces será suficiente mostrar que $\Gamma \vdash \psi$. (Incluso si x ocurre libre en Γ, se puede evitar la dificultad. Siempre habrá una variable y tal que $\Gamma \vdash \forall y\ \psi^x_y$ y $\forall y\ \psi^x_y \vdash \forall x\ \psi$. Véase el lema de reemplazo, ejercicio 9.)

3. Finalmente, supongamos que φ es la negación de otra fórmula.

3a. Si φ es $\neg(\psi \to \theta)$, entonces bastará mostrar que $\Gamma \vdash \psi$ y $\Gamma \vdash \neg\theta$ (por la regla T). Y esto siempre será posible.

3b. Si φ es $\neg\neg\psi$, entonces, desde luego, será suficiente mostrar que $\Gamma \vdash \psi$.

3c. El caso restante es donde φ es $\neg\forall x\, \psi$. Bastaría mostrar que $\Gamma \vdash \neg\, \psi^x_t$, donde t es algún término sustituible por x en ψ. (¿Por qué?) Desafortunadamente esto no siempre es posible. Hay casos en los que

$$\Gamma \vdash \neg\forall x\, \psi,$$

y aún así, para cada término t,

$$\Gamma \nvdash \neg\, \psi^x_t.$$

(Un ejemplo tal es $\Gamma = \emptyset$, $\psi = \neg\,(Px \rightarrow \forall y\, Py)$.) La contraposición es muy útil aquí;

$$\Gamma; \alpha \vdash \neg\forall x\, \psi$$

sii

$$\Gamma; \forall x\, \psi \vdash \neg\, \alpha.$$

(Una variante de esto es: $\Gamma; \forall y\; \alpha \vdash \neg\forall x\, \psi$ si $\Gamma; \forall x\; \psi \vdash \neg\, \alpha$.) Si todo lo demás falla, podemos intentar con reducción al absurdo.

Ejemplo (Q2a) Si x no ocurre libre en α, entonces

$$\vdash (\alpha \rightarrow \forall x\, \beta) \leftrightarrow \forall x\, (\alpha \rightarrow \beta).$$

Para probar esto, es suficiente mostrar (por la regla T) que

$$\vdash (\alpha \rightarrow \forall x\, \beta) \rightarrow \forall x\, (\alpha \rightarrow \beta)$$

y

$$\vdash \forall x\, (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \forall x\, \beta).$$

Para el primero, es suficiente (por los teoremas de la deducción y de generalización) mostrar que

$$\{(\alpha \rightarrow \forall x\, \beta), \alpha\} \vdash \beta.$$

Pero esto es fácil; $\forall x\, \beta \rightarrow \beta$ es un axioma.

Para obtener el inverso,

$$\vdash \forall x\, (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \forall x\, \beta),$$

es suficiente (por los teoremas de la deducción y de generalización) mostrar que

$$\{\forall x(\alpha \to \beta), \alpha\} \vdash \beta.$$

De nuevo, esto es fácil.

En el ejemplo anterior podemos reemplazar α por $\neg\alpha$, β por $\neg\beta$ y usar la tautología de contraposición (entre otras cosas) para obtener el hecho relacionado:

(Q3B) Si x no ocurre libre en α, entonces

$$\vdash (\exists x\, \beta \to \alpha) \leftrightarrow \forall x(\beta \to \alpha).$$

Tal vez el lector quiera convencerse por sí mismo de que la fórmula anterior *es* válida.

Con frecuencia, un estilo abreviado es útil para poner por escrito una prueba de deducibilidad, como en el ejemplo siguiente.

EJEMPLO (EC2) $\forall x\, \forall y\, (x = y \to y = x)$.

Demostración

1. $\vdash x = y \to x = x \to y = x$. Ax 6.
2. $\vdash x = x$. Ax 5.
3. $\vdash x = y \to y = x$. 1, 2; T.
4. $\vdash \forall x\, \forall y\, (x = y \to y = x)$. 3; gen^2. ⊣

En la línea 1, "Ax 6" significa que la fórmula pertenece al grupo 6 de axiomas. En la línea 3, "1, 2; T" significa que esta línea fue obtenida de las líneas 1 y 2 por la regla T. En la línea 4, "3; gen^2" significa que el teorema de generalización puede aplicarse dos veces a la línea 3 para producir la línea 4. En la misma tendencia, escribimos "MP", "ded", y "RAA" para referirnos respectivamente a modus ponens, al teorema de la deducción y a reducción al absurdo.

Se debe poner énfasis en que las cuatro líneas numeradas de arriba no constituyen una deducción de $\forall x\, \forall y\, (x = y \to$

$y = x$). En lugar de eso, forman una demostración (en el metalenguaje que con poca justificación seguimos llamando español) de que dicha deducción existe. La deducción más corta de $\forall x \forall y\, (x = y \to y = x)$ que el autor conoce es una sucesión de diecisiete fórmulas.

EJEMPLO $\vdash x = y \to \forall z\, Pxz \to \forall z\, Pyz$.

Demostración

1. $\vdash x = y \to Pxz \to Pyz$. Ax 6.
2. $\vdash \forall z Pxz \to Pxz$. Ax 2.
3. $\vdash x = y \to \forall z Pxz \to Pyz$. 1, 2; T.
4. $\{x = y,\ \forall z Pxz\} \vdash Pyz$. 3; MP[2].
5. $\{x = y,\ \forall z Pxz\} \vdash \forall z\, Pyz$. 4; gen.
6. $\vdash x = y \to \forall z Pxz \to \forall z Pyz$. 5; ded[2]. ⊣

EJEMPLO (EC5) Sea f un símbolo de función de dos argumentos. Entonces

$$\vdash \forall x_1 \forall x_2 \forall y_1 \forall y_2\, (x_1 = y_1 \to x_2 = y_2 \to f x_1 x_2 = f y_1 y_2).$$

Demostración Dos elementos del grupo 6 de axiomas son

$$x_1 = y_1 \to f x_1 x_2 = f x_1 x_2 \to f x_1 x_2 = f y_1 x_2,$$
$$x_2 = y_2 \to f x_1 x_2 = f y_1 x_2 \to f x_1 x_2 = f y_1 y_2.$$

De $\forall x\, x = x$ (del grupo 5 de axiomas) deducimos

$$f x_1 x_2 = f x_1 x_2.$$

Las tres fórmulas mostradas implican tautológicamente:

$$x_1 = y_1 \to x_2 = y_2 \to f x_1 x_2 = f y_1 y_2. \qquad ⊣$$

EJEMPLO

(a) $\{\forall x (Px \to Qx),\ \forall z\ Pz\} \vdash Qc$. No es difícil mostrar que tal deducción existe. La deducción en sí misma consta de siete fórmulas.

(b) $\{\forall x(Px \to Qx), \forall z\ Pz\} \vdash Qy$. Ésta es como en (a). Lo que nos interesa aquí es que podemos utilizar la *misma* deducción de siete elementos, reemplazando c por y en todas partes.

(c) $\{\forall x(Px \to Qx), \forall z\ Pz\} \vdash \forall y\ Qy$. Esto se sigue de (b) por el teorema de generalización.

(d) $\{\forall x(Px \to Qx), \forall z\ Pz\} \vdash \forall x\ Qx$. Esto se sigue de (c) usando $\forall y\ Qy \vdash \forall x\ Qx$.

Las partes (a) y (b) del ejemplo anterior ilustran un tipo de posibilidad de intercambio entre símbolos de constante y variables libres. Este tipo de intercambio es la base de la siguiente variante del teorema de generalización, de la cual es ejemplo la parte (c). El Corolario 24G cubre la parte (d). φ^c_y es, por supuesto, el resultado de reemplazar c por y en φ.

Teorema 24F (Generalización sobre constantes) Supongamos que $\Gamma \vdash \varphi$ y que c es un símbolo de constante que no ocurre en Γ. Entonces hay una variable y (que no ocurre en φ) tal que $\Gamma \vdash \forall y\ \varphi^c_y$. Además, hay una deducción de $\forall y\ \varphi^c_y$ a partir de Γ en la que c no ocurre.

Demostración Sea $\langle \alpha_0, \ldots, \alpha_n \rangle$ una deducción de φ a partir de Γ. (Por lo tanto $\alpha_n = \varphi$.) Sea y la primera variable que no ocurra en ninguna de las α_i. Afirmamos que

$$\langle (\alpha_0)^c_y, \ldots, (\alpha_n)^c_y \rangle \qquad (*)$$

es una deducción de φ^c_y a partir de Γ. Así que debemos verificar que cada $(\alpha_k)^c_y$ está en $\Gamma \cup \Lambda$ o que se obtiene a partir de fórmulas anteriores por modus ponens.

Caso 1: $\alpha_k \in \Gamma$. Entonces c no ocurre en α_k. Así que $(\alpha_k)^c_y = \alpha_k$, que está en Γ.

Caso 2: α_k es un axioma lógico. Entonces $(\alpha_k)^c_y$ también es un axioma lógico. (Véase la lista de axiomas lógicos y nótese que la introducción de una nueva variable transformará un axioma lógico en otro axioma lógico.)

Caso 3: α_k se obtiene por modus ponens de α_i y α_j (que es $(\alpha_i \to \alpha_k)$) para i, j menores que k. Entonces

$(\alpha_j)_y^c = ((\alpha_i)_y^c \to (\alpha_k)_y^c)$. Así que $(\alpha_k)_y^c$ se obtiene de $(\alpha_i)_y^c$ y $(\alpha_j)_y^c$ por modus ponens.

Esto completa la prueba de que (*) anterior es una deducción de φ_y^c. Sea Φ el subconjunto finito de Γ que se usa en (*). Así, (*) es una deducción de φ_y^c a partir de Φ, y y no ocurre en Φ. Así que por el teorema de generalización, $\Phi \vdash \forall y\ \varphi_y^c$. Además, hay una deducción de $\forall y\ \varphi_y^c$, a partir de Φ en la que c no aparece. (Pues la prueba del teorema de generalización no agregó ningún nuevo símbolo a la deducción.) Ésta es también una deducción de $\forall y\, \varphi_y^c$ a partir de Γ. ⊣

A veces querremos aplicar este teorema en circunstancias en las que no se podría aplicar cualquier variable. En la versión siguiente se selecciona de antemano una variable x.

Corolario 24G Supongamos que $\Gamma \vdash \varphi_c^x$, donde el símbolo de constante c no ocurre en Γ ni en φ. Entonces $\Gamma \vdash \forall x\ \varphi$, y hay una deducción de $\forall x\ \varphi$ a partir de Γ, en la que c no ocurre.

Demostración Por el teorema anterior, tenemos una deducción (sin c) a partir de Γ de $\forall y\, ((\varphi_c^x)_y^c)$, donde y no ocurre en φ_c^x. Pero ya que c no ocurre en φ,

$$(\varphi_c^x)_y^c = \varphi_y^x.$$

Falta demostrar que $\forall y\ \varphi_y^x \vdash \forall x\ \varphi$. Podemos hacer esto fácilmente si sabemos que

$$(\forall y\ \varphi_y^x) \to \varphi$$

es un axioma. Esto es, x debe ser sustituible por y en φ_y^x, y $(\varphi_y^x)_x^y$ tiene que ser φ. Esto queda razonablemente claro; los detalles pueden consultarse en el lema de reemplazo (Ejercicio 9). ⊣

Corolario 24H (Regla IE) Supongamos que el símbolo de constante c no ocurre en φ ni en ψ ni en Γ, y que

$$\Gamma; \varphi_c^x \vdash \psi.$$

Entonces

$$\Gamma; \exists x\, \varphi \vdash \psi$$

y hay una deducción de ψ a partir de $\Gamma; \exists x \varphi$ en la que c no ocurre.

Demostración Por contraposición tenemos que

$$\Gamma; \neg \psi \vdash \neg \varphi^x_c.$$

Así, por el corolario anterior obtenemos

$$\Gamma; \neg \psi \vdash \forall x \neg \varphi.$$

Al aplicar la contraposición nuevamente, tenemos el resultado deseado. ⊣

"IE" abrevia "instanciación existencial", un ejemplo de terminología tradicional.

No tendremos oportunidad de usar la regla IE en ninguna de nuestras demostraciones, pero puede ser útil en los ejercicios. Es la contraparte formal del razonamiento: "Sabemos que existe una x tal que __x__. Así que llamémosla c. Ahora, a partir de __c__ podemos probar ψ." Pero nótese que la regla IE *no* afirma que $\exists x\, \varphi \vdash \varphi^x_c$, lo que de hecho suele ser falso.

EJEMPLO revisado. $\vdash \exists x \forall y\, \varphi \to \forall y \exists x\, \varphi$.

Por el teorema de la deducción, es suficiente mostrar que

$$\exists x \forall y\, \varphi \vdash \forall y \exists x\, \varphi.$$

Por la regla IE, es suficiente mostrar que

$$\forall y\, \varphi^x_c \vdash \forall y \exists x\, \varphi,$$

donde c es una nueva constante para el lenguaje. Por el teorema de generalización, basta mostrar que

$$\forall y\, \varphi^x_c \vdash \exists x\, \varphi.$$

Ya que $\forall y\, \varphi^x_c \vdash \varphi^x_c$, es suficiente mostrar que

$$\varphi^x_c \vdash \exists x\, \varphi.$$

Por contraposición, esto es equivalente a

$$\forall x \neg \varphi \vdash \neg \varphi^x_c,$$

lo cual es trivial (por el grupo 2 de axiomas y modus ponens).

Ahora, podemos ver más o menos cómo se construyó nuestra lista particular de axiomas lógicos. Se incluyeron las tautologías para manejar los símbolos de conectivo proposicional. (En este momento podríamos ahorrarnos mucho si usáramos únicamente algunas de las tautologías.) El grupo 2 de axiomas refleja el significado que se pretende que tenga el símbolo de cuantificador. Después, para poder probar el teorema de generalización, agregamos los grupos de axiomas 3 y 4 e hicimos los ajustes para que las generalizaciones de axiomas fueran axiomas.

Los grupos de axiomas 5 y 6 resultarán ser justo lo suficiente para probar las propiedades cruciales de la igualdad; véase la subsección sobre igualdad.

Como lo probaremos en la sección 5 de este capítulo, cada axioma lógico es una fórmula válida. Podría parecer más sencillo usar como axiomas lógicos el conjunto de *todas* las fórmulas válidas; pero hay dos objeciones (relacionadas entre sí) contra esto. La primera es que el concepto de validez se definió *semánticamente*. Esto es, la definición hacía referencia a significados posibles (es decir, estructuras) para el lenguaje y para el concepto de verdad en una estructura. Para nuestros propósitos actuales (es decir, probar que el conjunto de las fórmulas válidas es efectivamente numerable) necesitamos una clase Λ con una definición *sintáctica* finitaria. Esto es, la definición de Λ involucra únicamente conceptos concernientes a la disposición de los símbolos en los axiomas lógicos; no hay ninguna referencia a conceptos de verdad en estructuras. Una segunda objeción en contra de que se incluyan todas las fórmulas válidas como axiomas es que nosotros preferimos un conjunto Λ decidible, y el conjunto de las fórmulas válidas no es decidible.

Variantes alfabéticas

Con frecuencia, cuando analizamos una fórmula como

$$\forall x(x \neq \mathbf{0} \to \exists y\, x = \mathbf{S}y)$$

no estamos interesados particularmente en elegir las variables x y y. Queremos que $\langle x, y\rangle$ sea un par de variables distintas; pero no suele haber diferencia si el par es $\langle v_4, v_9\rangle$ o $\langle v_8, v_1\rangle$.

Ahora bien, cuando llega el momento de sustituir un término t en una fórmula, entonces elegir variables cuantificadas puede determinar que t sea sustituible o no. En esta subsección discutiremos qué hacer cuando la sustituibilidad falla. Como se verá, la dificultad siempre se podrá superar jugando adecuadamente con las variables cuantificadas.

Por ejemplo, supongamos que queremos mostrar que

$$\vdash \forall x \forall y\, Pxy \to \forall y\, Pyy.$$

La dificultad aquí es que y no es sustituible por x en $\forall y\; Pxy$, así que el enunciado anterior no está en el grupo 2 de axiomas. Este inconveniente es resultado de una elección desafortunada de variables. Por ejemplo, mostrar que

$$\vdash \forall x \forall z\, Pxz \to \forall y\, Pyy$$

no supone tales dificultades; así que podemos resolver nuestro problema original si sabemos que

$$\vdash \forall x \forall y\, Pxy \to \forall x \forall z\, Pxz,$$

lo cual, de nuevo, no implica ninguna dificultad.

Esta estrategia un tanto indirecta (de interpolar $\forall x\; \forall z\; Pxz$ entre $\forall x\; \forall y\; Pxy$ y $\forall y\; Pyy$ es típica de cierta clase de problemas. Digamos que deseamos sustituir un término t por x en una fórmula φ. Si de hecho t no es sustituible allí, entonces reemplazamos $\forall x\; \varphi$ por $\forall x\; \varphi'$ donde t sí es sustituible por x en φ'. En el ejemplo anterior, φ es $\forall y\; Pxy$ y φ' es $\forall z\; Pxz$. En general, φ' sólo se diferencia de φ en la elección de las variables cuantificadas. Pero φ' deberá formarse de una manera razonable para ser lógicamente equivalente a φ. Por ejemplo,

no sería razonable sustituir $\forall y\, Pxy$ por $\forall x\, Pxx$ ni $\forall y\, \forall z\, Qxyz$ por $\forall z\, \forall z\, Qxzz$.

Teorema 24I (Existencia de variantes alfabéticas) Sean φ una fórmula, t un término y x una variable. Entonces podemos encontrar una fórmula φ' (que difiere de φ sólo en la elección de las variables cuantificadas) tal que

(a) $\varphi \vdash \varphi'$ y $\varphi' \vdash \varphi$;
(b) t es sustituible por x en φ'.

Demostración Consideramos que t y x son fijos, y construimos φ' por recursión sobre φ. Los primeros casos son sencillos: para φ atómica, tomamos $\varphi' = \varphi$, y después $(\neg\varphi)' = (\neg\varphi')$, $(\varphi \to \psi)' = (\varphi' \to \psi')$. Pero consideremos ahora la elección de $(\forall y\, \varphi)'$.

Si y no ocurre en t, o si $y = x$, entonces simplemente podemos tomar $(\forall y\, \varphi)' = \forall y\, \varphi'$; sin embargo, para el caso general debemos cambiar la variable.

Elijamos una variable z que no ocurra en φ' ni en t ni en x. Después definimos $(\forall y\, \varphi)' = \forall z\, (\varphi')^y_z$. Para verificar que (b) se cumple, hacemos notar que z no ocurre en t y que t es sustituible por x en φ' (por la hipótesis inductiva). Por lo tanto (ya que $x \neq z$), t también es sustituible por x en $(\varphi')^y_z$. Para verificar que (a) se cumple, calculamos:

$\varphi \vdash \varphi'$	por la hipótesis inductiva;
$\therefore\ \forall y\, \varphi \vdash \forall y\, \varphi'$.	
$\forall y\, \varphi' \vdash (\varphi')^y_z$	ya que z no ocurre en φ';
$\therefore\ \forall y\, \varphi' \vdash \forall z\, (\varphi')^y_z$	por generalización;
$\therefore\ \forall y\, \varphi \vdash \forall z\, (\varphi')^y_z$.	

En la otra dirección,

$\forall z (\varphi')^y_z \vdash ((\varphi')^y_z)^z_y$,	que es φ' por el ejercicio 9;
$\varphi' \vdash \varphi$;	por la hipótesis inductiva;
$\therefore\ \forall z\, (\varphi')^y_z \vdash \varphi$	
$\therefore\ \forall z\, (\varphi')^y_z \vdash \forall y\, \varphi$	por generalización.

El último paso usa el hecho de que y no ocurre libre en $(\varphi')^y_z$ a menos que $y = z$, y por lo tanto no ocurre libre en $\forall z\, (\varphi')^y_z$ en ningún caso. ⊣

Las fórmulas φ' construidas como en la demostración de este teorema se llamarán *variantes alfabéticas* de φ. La moraleja del teorema es la siguiente: no debemos desanimarnos si falla la posibilidad de sustituir; la variante alfabética adecuada evitará la dificultad.

Igualdad

A continuación se presenta una lista (suponiendo que nuestro lenguaje incluye =) de ciertos datos sobre igualdad que serán necesarios en la siguiente sección. Para empezar, la relación definida por $v_1 = v_2$ es reflexiva, simétrica y transitiva (es decir, es una relación de equivalencia):

$$\text{Ec 1:} \quad \vdash \forall x\, x = x.$$

Demostración Grupo 5 de axiomas. ⊣

$$\text{Ec 2:} \quad \vdash \forall x\, \forall y\, (x = y \to y = x).$$

Demostración Es el ejemplo Ec2 (p. 180). ⊣

$$\text{Ec3:} \quad \vdash \forall x \forall y \forall z (x = y \to y = z \to x = z).$$

Demostración Ejercicio 11. ⊣

Además necesitaremos saber que la igualdad es compatible con los símbolos de predicado y de función:

Ec 4 (para un símbolo de predicado P de dos argumentos):

$$\vdash \forall x_1\, \forall x_2\, \forall y_1\, \forall y_2\, (x_1 = y_1 \to x_2 = y_2 \to Px_1x_2 \to Py_1y_2).$$

De manera similar para los símbolos de predicado de n argumentos.

Demostración Es suficiente mostrar que

$$\{x_1 = y_1,\ x_2 = y_2,\ Px_1x_2\} \vdash Py_1y_2.$$

Esto se obtiene aplicando modus ponens a los siguientes dos elementos del grupo 6 de axiomas:

$$x_1 = y_1 \to Px_1x_2 \to Py_1x_2,$$
$$x_2 = y_2 \to Py_1x_2 \to Py_1y_2. \qquad \dashv$$

Ec 5 (para un símbolo de función f de dos argumentos):

$$\vdash \forall x_1 \forall x_2 \forall y_1 \forall y_2 (x_1 = y_1 \to x_2 = y_2 \to fx_1x_2 = fy_1y_2).$$

De manera similar para los símbolos de función de n argumentos.

Demostración Ejemplo Ec5 (p. 181). $\dashv$

Comentarios finales

Un libro de lógica con un enfoque tradicional autosuficiente bien podría comenzar con esta sección sobre un cálculo deductivo. Un libro así primeramente establecería los axiomas lógicos y las reglas de inferencia y explicaría que éstos son aceptables para personas razonables. Después procedería a mostrar que muchas fórmulas son deducibles (o deducibles a partir de ciertos axiomas no lógicos, como los axiomas de la teoría de los conjuntos).

Nuestro punto de vista es muy diferente. Nosotros estudiamos, entre otras cosas, los hechos sobre el procedimiento descrito en el párrafo anterior. Y para eso utilizamos cualquier razonamiento matemático correcto, a sabiendas o no de que dicho razonamiento tiene sus equivalentes en el cálculo deductivo que ahora estudiamos.

La figura 8 tiene por objeto ilustrar la separación entre (a) el nivel en el cual realizamos nuestro razonamiento y demostramos nuestros resultados, y (b) el nivel del cálculo deductivo que estudiamos.

Ejercicios

1. Para un término u, sea u_t^x la expresión obtenida a partir de u al reemplazar la variable x por el término t. Reformule esta definición sin usar ninguna forma de la palabra

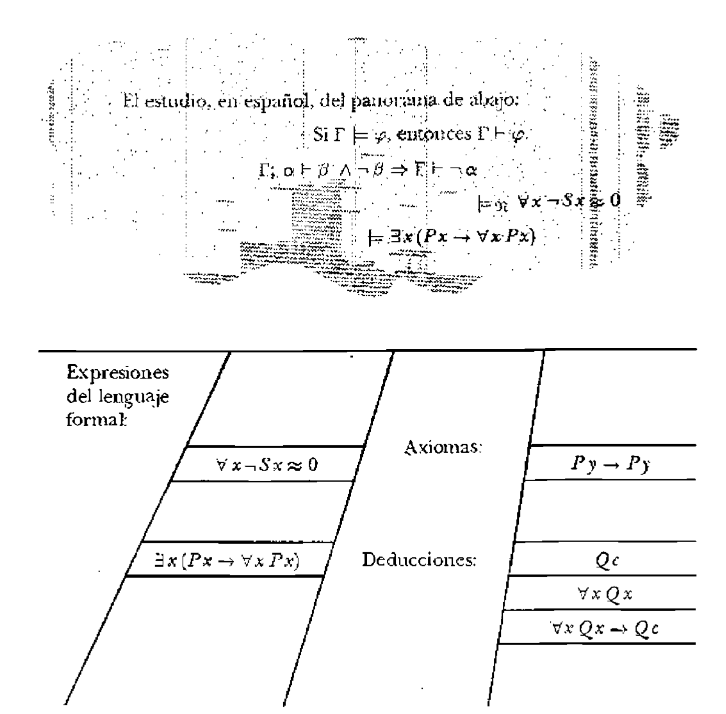


FIGURA 8. *Arriba se observa el metalenguaje en el cual estudiamos el lenguaje objeto de abajo.*

"reemplazo" o sus sinónimos. *Sugerencia:* Utilice recursión sobre u. (Observe que a partir de la nueva definición queda claro que u_t^x es un término.)

2. ¿A qué grupo de axiomas pertenecen, si es que pertenecen a alguno, las siguientes fórmulas?

   (a) $[(\forall x\, Px \to \forall y\, Py) \to Pz] \to [\forall x\, Px \to (\forall y\, Py \to Pz)]$.

   (b) $\forall y\, [\forall x(Px \to Px) \to (Pc \to Pc)]$.

   (c) $\forall x \exists y\, Pxy \to \exists y\, Pyy$.

3. (a) Sea $\mathfrak{A}$ una estructura y sea $s : V \to |\mathfrak{A}|$. Defina una asignación de verdad v sobre el conjunto de las fórmulas primas usando

$$v(\alpha) = T \quad \text{sii} \quad \models_{\mathfrak{A}} \alpha[s].$$

Muestre que para cualquier fórmula (prima o no prima),

$$\bar{v}(\alpha) = T \quad \text{sii} \quad \models_{\mathfrak{A}} \alpha[s].$$

Observación: Este resultado refleja el hecho de que $\neg$ y $\to$ se trataron en el capítulo II de la misma manera que en el capítulo I.

(b) Concluya que si Γ implica tautológicamente φ, entonces Γ implica lógicamente φ.

4. Dé una deducción (a partir de $\emptyset$) de $\forall x\, \varphi \to \exists x\, \varphi$. (Nótese que no sólo se deberá probar que dicha deducción existe. Se está pidiendo más bien que se escriba la deducción completa.)

5. Encuentre una función f tal que si una fórmula φ tiene una deducción de tamaño n a partir de un conjunto Γ, y si x no ocurre libre en Γ, entonces $\forall x\, \varphi$ tiene una deducción a partir de Γ de tamaño $f(n)$. Cuanto más despacio crezca su función, será mejor.

6. (a) Muestre que si $\vdash \alpha \to \beta$, entonces $\vdash \forall x\, \alpha \to \forall x\, \beta$.

(b) Muestre que en general no es verdad que $\alpha \to \beta \models \forall x\, \alpha \to \forall x\, \beta$.

7. (a) Muestre que $\vdash \exists x\, (Px \to \forall x\, Px)$.

(b) Muestre que $\{Qx, \forall y\, (Qy \to \forall z\, Pz)\} \vdash \forall x\, Px$.

8. (Q2b) Suponga que x no ocurre libre en α. Muestre que

$$\vdash (\alpha \to \exists x\, \beta) \leftrightarrow \exists x (\alpha \to \beta).$$

También muestre, suponiendo lo mismo, que tenemos Q3a:

$$\vdash (\forall x\, \beta \to \alpha) \leftrightarrow \exists x\, (\beta \to \alpha).$$

9. (Lema de reemplazo) (a) Muestre mediante un ejemplo que $(\varphi_y^x)_x^y$ en general no es igual a φ. Y que es posible tanto que x ocurra en $(\varphi_y^x)_x^y$ en un lugar donde no ocurre en φ, como que x ocurra en φ en un lugar donde no ocurre en $(\varphi_y^x)_x^y$.

   (b) Muestre que si y no ocurre en φ, entonces x es sustituible por y en φ_y^x y $(\varphi_y^x)_x^y = \varphi$. *Sugerencia*: Use inducción sobre φ.

10. Muestre que

$$\forall x \forall y\, Pxy \vdash \forall y \forall x\, Pyx.$$

11. (Ec 3) Muestre que

$$\vdash \forall x \forall y \forall z\, (x = y \to y = z \to x = z).$$

12. Muestre que cualquier conjunto de fórmulas Γ consistente puede extenderse a un conjunto consistente Δ con la propiedad de que para cualquier fórmula α, o bien $\alpha \in \Delta$ o $(\neg \alpha) \in \Delta$. (Suponga que el lenguaje es numerable. No use el teorema de compacidad de la lógica de enunciados.)

13. Muestre que $\vdash Py \leftrightarrow \forall x\,(x = y \to Px)$.

    Observaciones: De forma más general, si t es sustituible por x en φ y x no ocurre en t, entonces

$$\vdash [\varphi_t^x \leftrightarrow \forall x\,(x = t \to \varphi)].$$

   De esta manera, la fórmula $\forall x\,(x = t \to \varphi)$ ofrece un modo alternativo para la sustitución φ_t^x.

14. Muestre que $\vdash (\forall x((\neg Px) \to Qx) \to \forall y((\neg Qy) \to Py))$.

15. Muestre que existen las deducciones (a partir de $\emptyset$) de las fórmulas siguientes:

    (a) $\exists x\, \alpha \vee \exists x\, \beta \leftrightarrow \exists x\,(\alpha \vee \beta)$.

    (b) $\forall x\, \alpha \vee \forall x\, \beta \to \forall x\,(\alpha \vee \beta)$.

16. Muestre que existen las deducciones (a partir de $\emptyset$) de las fórmulas siguientes:

    (a) $\exists x(\alpha \wedge \beta) \to \exists x\, \alpha \wedge \exists x\, \beta$.

    (b) $\forall x(\alpha \wedge \beta) \leftrightarrow \forall x\, \alpha \wedge \forall x\, \beta$.

17. Muestre que existen las deducciones (a partir de $\emptyset$) de las fórmulas siguientes:

    (a) $\forall x(\alpha \to \beta) \to (\exists x\, \alpha \to \exists x\, \beta)$.

    (b) $\exists x(Py \wedge Qx) \leftrightarrow Py \wedge \exists x\, Qx$.

5. *Teoremas de correctud y de completud*

En esta sección estableceremos dos teoremas importantes: la correctud de nuestro cálculo deductivo ($\Gamma \vdash \varphi \Rightarrow \Gamma \models \varphi$) y su completud ($\Gamma \models \varphi \Rightarrow \Gamma \vdash \varphi$). Luego nos será posible obtener varias conclusiones interesantes (incluyendo los teoremas de compacidad y de numerabilidad). Aunque nuestro cálculo deductivo fue elegido de una manera un tanto arbitraria, el hecho significativo es que *algún* cálculo deductivo así es correcto y completo. Esto deberá estimular al "matemático activo" interesado en la existencia de demostraciones a partir de axiomas; véase la subsección "Retrospectiva" de la sección 6 de este capítulo.

Teorema de correctud Si $\Gamma \vdash \varphi$, entonces $\Gamma \models \varphi$.

El teorema de correctud nos dice que nuestras deducciones nos llevan únicamente a conclusiones "correctas" (¡de otra manera las deducciones no tendrían sentido!). La idea de la demostración es que los axiomas lógicos son lógicamente implicados por cualquier cosa, y que el modus ponens preserva las implicaciones lógicas.

Lema 25A Todo axioma lógico es válido.

Demostración del teorema de correctud, suponiendo el lema Mostramos por inducción que cualquier fórmula φ deducible a partir de Γ es implicada lógicamente por Γ.

Caso 1: φ es un axioma lógico. Entonces por el lema $\models \varphi$, por tanto, *a fortiori* $\Gamma \models \varphi$.

Caso 2: $\varphi \in \Gamma$. Entonces claramente $\Gamma \models \varphi$.

Caso 3: φ se obtiene por modus ponens de ψ y $\psi \to \varphi$, de donde (por hipótesis inductiva) $\Gamma \models \psi$ y $\Gamma \models (\psi \to \varphi)$. Luego se sigue inmediatamente que $\Gamma \models \varphi$. ⊣

Por supuesto, queda pendiente demostrar el lema. Por el ejercicio 6 de la sección 2 de este capítulo, sabemos que cualquier generalización de una fórmula válida es válida. Así que basta considerar únicamente los axiomas lógicos que no sean generalizaciones de otros axiomas. Examinaremos los diversos grupos de axiomas por orden de complejidad.

Grupo 3 de axiomas: Véase el ejercicio 3 de la sección 2 de este capítulo.

Grupo 4 de axiomas: Véase el ejercicio 4 de la sección 2 de este capítulo.

Grupo 5 de axiomas: Trivial. $\mathfrak{A}$ satisface $x = x$ con s sii $s(x) = s(x)$, lo cual siempre es verdadero.

Grupo 1 de axiomas: Por el ejercicio 3 de la sección anterior sabemos que si $\emptyset$ implica tautológicamente α, entonces $\emptyset \models \alpha$. Y eso es justamente lo que necesitamos.

Grupo 6 de axiomas (véase como ejemplo el ejercicio 5 de la sección 2 de este capítulo): Supongamos que α es atómica y que α' se obtiene a partir de α al reemplazar x por y en algunos lugares. Es suficiente mostrar que

$$\{x = y,\ \alpha\} \models \alpha'.$$

Así que tomemos cualesquiera $\mathfrak{A}$ y s tales que

$$\models_{\mathfrak{A}} x = y\,[s], \quad \text{es decir, } s(x) = s(y).$$

Entonces, cualquier término t tiene la propiedad de que si t' se obtiene de t al reemplazar x por y en algunos lugares, entonces $\bar{s}(t) = \bar{s}(t')$. Esto es obvio; una demostración completa utilizaría inducción sobre t.

Si α es $t_1 = t_2$, entonces α' deberá ser $t'_1 = t'_2$, donde t'_i se obtiene a partir de t_i como se describió.

$$\begin{aligned} \models_{\mathfrak{A}} \alpha[s] \quad &\text{sii} \quad \bar{s}(t_1) = \bar{s}(t_2), \\ &\text{sii} \quad \bar{s}(t'_1) = \bar{s}(t'_2), \\ &\text{sii} \quad \models_{\mathfrak{A}} \alpha'[s]. \end{aligned}$$

De manera similar, si α es $Pt_1 \cdots t_n$, entonces α' es $Pt'_1 \cdots t'_n$, y se aplica un argumento análogo.

Finalmente, llegamos al grupo 2 de axiomas. Será útil considerar primero un caso sencillo: mostraremos que $\forall x\, Px \rightarrow Pt$ es válida. Supongamos que

$$\models_{\mathfrak{A}} \forall x\, Px[s].$$

Entonces, para cualquier d en $|\mathfrak{A}|$,

$$\models_{\mathfrak{A}} Px[s(x \mid d)].$$

Así que en particular podemos tomar $d = \bar{s}(t)$:

$$\models_{\mathfrak{A}} Px[s(x \mid \bar{s}(t))]. \qquad \text{(a)}$$

Esto es equivalente (por la definición de satisfacción para fórmulas atómicas) a

$$\bar{s}(t) \in P^{\mathfrak{A}},$$

lo cual a su vez es equivalente a

$$\models_{\mathfrak{A}} Pt[s]. \qquad \text{(b)}$$

Para que este argumento se pueda aplicar a un caso no atómico, necesitamos una manera de pasar de (a) a (b). Esto se obtendrá con el lema de sustitución que aparece abajo, el cual establece que

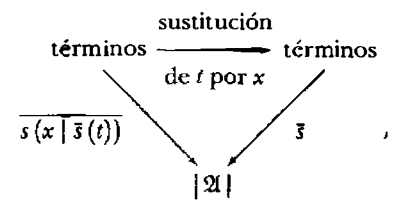
$$\models_{\mathfrak{A}} \varphi[s(x \mid \bar{s}(t))] \quad \text{sii} \quad \models_{\mathfrak{A}} \varphi^x_t[s]$$

siempre que t sea sustituible por x en φ.

Consideremos una $\mathfrak{A}$ y una s fijas. Para cualquier término u, sea u^x_t el resultado de reemplazar la variable x en u por el término t.

Lema 258 $\bar{s}(u^x_t) = \overline{s(x \mid \bar{s}(t))}(u)$.

Esto parece más complicado de lo que en realidad es. Esta expresión afirma que se puede realizar una sustitución ya sea en el término u o en s, con resultados equivalentes. En seguida se muestra el diagrama conmutativo correspondiente.



Demostración Por inducción sobre el término u. Si u es un símbolo de constante o una variable diferente de x, entonces $u_t^x = u$ y la ecuación deseada se reduce a $\bar{s}(u) = \bar{s}(u)$. Si $u = x$, la ecuación se reduce entonces a $\bar{s}(t) = \bar{s}(t)$. El paso inductivo, aunque un tanto complicado de escribir, es matemáticamente trivial. ⊣

El lema de sustitución en esencialmente similar; establece que se puede realizar una sustitución ya sea dentro de φ o en s, con resultados equivalentes. Véase un ejemplo en el ejercicio 10 de la sección 2 de este capítulo.

Lema de sustitución Si el término t es sustituible por la variable x en la fórmula φ, entonces

$$\models_{\mathfrak{A}} \varphi_t^x[s] \quad \text{sii} \quad \models_{\mathfrak{A}} \varphi[s(x \mid \bar{s}(t))].$$

Demostración Usamos inducción sobre φ para mostrar que lo anterior se cumple para toda s.

Caso 1: φ es atómica. Entonces la conclusión se sigue del lema anterior. Por ejemplo, si φ es Pu para algún término u, entonces

$$\begin{aligned} \models_{\mathfrak{A}} Pu_t^x[s] \quad & \text{sii} \quad \bar{s}(u_t^x) \in P^{\mathfrak{A}}, \\ & \text{sii} \quad \overline{s(x \mid \bar{s}(t))}(u) \in P^{\mathfrak{A}} \quad \text{por el lema 25B}, \\ & \text{sii} \quad \models_{\mathfrak{A}} Pu[s(x \mid \bar{s}(t))]. \end{aligned}$$

Caso 2: φ es $\neg\psi$ o $\psi \to \theta$. Entonces se sigue inmediatamente la conclusión para φ a partir de la hipótesis inductiva para ψ y θ.

Caso 3: φ es $\forall y\, \psi$, y x no ocurre libre en φ. Entonces s y $s(x \mid \bar{s}(t))$ coinciden en todas las variables que

ocurren libres en φ. Y también φ_t^x es simplemente φ, así que la conclusión es inmediata.

Caso 4: φ es $\forall y\ \psi$, y x *sí* ocurre libre en φ. Debido a que t es sustituible por x en φ, sabemos que y no ocurre en t y que t es sustituible por x en ψ (véase la definición de "sustituible"). Por la primera de esas dos cosas,

$$\bar{s}(t) = \overline{s(y \mid d)}(t) \qquad (*)$$

para cualquier d en $|\mathfrak{A}|$. Ya que $x \neq y$, $\varphi_t^x = \forall y\ \psi_t^x$.

$\models_{\mathfrak{A}} \varphi_t^x[s]$ sii para cada d, $\models_{\mathfrak{A}} \psi_t^x[s(y \mid d)]$,
sii para cada d, $\models_{\mathfrak{A}} \psi[s(y \mid d)(x \mid \bar{s}(t))]$ por la hipótesis inductiva y (*),
sii $\models_{\mathfrak{A}} \varphi[s(x \mid \bar{s}(t))]$.

Así, por inducción, el lema se cumple para toda φ. ⊣

Grupo 2 de axiomas: Supongamos que t es sustituible por x en φ. Supongamos que $\mathfrak{A}$ satisface $\forall x\ \varphi$ con s. Necesitamos mostrar que $\models_{\mathfrak{A}} \varphi_t^x[s]$. Sabemos que para cualquier d en $|\mathfrak{A}|$,

$$\models_{\mathfrak{A}} \varphi[s(x \mid d)].$$

En particular, sea $d = \bar{s}(t)$:

$$\models_{\mathfrak{A}} \varphi[s(x \mid \bar{s}(t))];$$

así, por el lema de sustitución,

$$\models_{\mathfrak{A}} \varphi_t^x[s].$$

De aquí que $\forall x\ \varphi \to \varphi_t^x$ es válida.

Esto completa la demostración de que todos los axiomas lógicos son válidos. Y así queda demostrado el teorema de correctud.

Corolario 25C Si $\vdash (\varphi \leftrightarrow \psi)$, entonces φ y ψ son lógicamente equivalentes.

Corolario 25D Si φ' es una variante alfabética de φ (véase el teorema 24I), entonces φ y φ' son lógicamente equivalentes.

Recuerde que un conjunto Γ es consistente sii no hay ninguna fórmula φ tal que $\Gamma \vdash \varphi$ y $\Gamma \vdash \neg\varphi$. Definimos que Γ es *satisfactible* sii hay algunas $\mathfrak{A}$ y s tales que $\mathfrak{A}$ satisface a cada elemento de Γ con s.

Corolario 25E Si Γ es satisfactible, entonces Γ es consistente.

Este corolario es de hecho equivalente al teorema de corrección, y se invita al lector a que lo verifique.

El teorema de completud es el inverso del teorema de corrección y es un resultado más profundo.

Teorema de completud (Gödel, 1930)

(a) Si $\Gamma \models \varphi$, entonces $\Gamma \vdash \varphi$.

(b) Cualquier conjunto de fórmulas consistente es satisfactible.

De hecho, las partes (a) y (b) son equivalentes; véase el ejercicio 2. Así que basta demostrar la parte (b). Daremos una demostración para un lenguaje numerable; más tarde indicaremos qué modificaciones son necesarias para lenguajes de mayor cardinalidad. (Un lenguaje numerable es aquel con una cantidad numerable de símbolos, o de manera equivalente, por el teorema 0B, uno con una cantidad numerable de fórmulas.)

Las ideas de la demostración están relacionadas con las de la demostración del teorema de compacidad de la lógica de enunciados. Comenzamos con un conjunto consistente Γ. En los pasos 1–3 extendemos Γ a un conjunto Δ de fórmulas para el cual

(i) $\Gamma \subseteq \Delta$.

(ii) Δ es consistente y es maximal en el sentido de que para cualquier fórmula α, $\alpha \in \Delta$ o $(\neg\alpha) \in \Delta$.

(iii) Para cualesquiera fórmula φ y variable x, hay una constante c tal que

$$(\neg\forall x\,\varphi \rightarrow \neg\varphi^x_c) \in \Delta.$$

Después, en el paso 4 construimos una estructura $\mathfrak{A}$ en la cual se satisfacen las fórmulas de Γ que no contengan $=$. $|\mathfrak{A}|$ es el conjunto de términos, y para un símbolo de predicado P,

$$\langle t_1, \ldots, t_n \rangle \in P^{\mathfrak{A}} \quad \text{sii} \quad Pt_1 \cdots t_n \in \Delta.$$

Finalmente, en los pasos 5 y 6 cambiamos $\mathfrak{A}$ para que satisfaga las fórmulas que contienen el símbolo de igualdad.

Se sugiere que en una primera lectura se omitan los detalles que se dan para la mayoría de los pasos. Una vez que se tenga en mente un esquema claro, se deberá leer la demostración completa. (Los pasos que no están detallados se señalan con una barra en el margen izquierdo.)

Demostración Sea Γ un conjunto consistente de fórmulas en un lenguaje numerable. ⊣

Paso 1 Expanda el lenguaje añadiendo un conjunto infinito numerable de nuevos símbolos de constante. Luego Γ sigue siendo consistente como un conjunto de fórmulas en el nuevo lenguaje.

Detalles: Si no, entonces para alguna β hay una deducción (en el lenguaje expandido) de $(\beta \wedge \neg\beta)$ a partir de Γ. Esta deducción contiene únicamente una cantidad finita de nuevos símbolos de constante. Por el teorema de generalización a partir de constantes (teorema 24F), cada uno puede ser reemplazado por una variable. Entonces tenemos una deducción (en el lenguaje original) de $(\beta' \wedge \neg\beta')$ a partir de Γ. Esto contradice nuestra suposición de que Γ era consistente.

Paso 2 Para cada fórmula φ (en el nuevo lenguaje) y para cada variable x, agregamos a Γ la fórmula

$$\neg\forall x\, \varphi \rightarrow \neg\varphi^x_c,$$

donde c es uno de los nuevos símbolos de constante. (La idea es que c se ofrece para nombrar un contraejemplo de φ, si hay alguno.) Podemos hacer esto de manera tal que Γ, junto con el conjunto Θ de todas las fórmulas agregadas, siga siendo un conjunto consistente.

Detalles: Adoptamos una numeración fija de los pares $\langle \varphi, x \rangle$ donde φ es una fórmula (del lenguaje expandido) y x es una variable:

$$\langle \varphi_1, x_1 \rangle, \langle \varphi_2, x_2 \rangle, \langle \varphi_3, x_3 \rangle, \ldots$$

Esto es posible, ya que el lenguaje es numerable. Sea θ_1

$$\neg \forall x_1 \varphi_1 \rightarrow \neg \varphi_1{}_{c_1}^{x_1},$$

donde c_1 es el primero de los nuevos símbolos de constante que no ocurren en φ_1. Luego seguimos con $\langle \varphi_2, x_2 \rangle$ y definimos θ_2. En general, θ_n es

$$\neg \forall x_n \, \varphi_n \rightarrow \neg \varphi_n{}_{c_n}^{x_n},$$

donde c_n es el primero de los símbolos de constante que no ocurren en φ_n ni en θ_k para ninguna $k < n$.

Sea Θ el conjunto $\{\theta_1, \theta_2, \ldots\}$. Afirmamos que $\Gamma \cup \Theta$ es consistente. Si no, entonces (como las deducciones son finitas), para alguna $m \geq 0$,

$$\Gamma \cup \{\theta_1, \ldots, \theta_m, \theta_{m+1}\}$$

es inconsistente. Tomemos la mínima m tal. Entonces, por RAA

$$\Gamma \cup \{\theta_1, \ldots, \theta_m\} \vdash \neg \theta_{m+1}.$$

Ahora bien, θ_{m+1} es

$$\neg \forall x \varphi \rightarrow \neg \varphi_c^x$$

para ciertos x, φ y c. Así que, por la regla T, obtenemos el par siguiente:

$$\begin{array}{l} \Gamma \cup \{\theta_1, \ldots, \theta_m\} \vdash \neg \forall x \, \varphi \\ \Gamma \cup \{\theta_1, \ldots, \theta_m\} \vdash \varphi_c^x. \end{array} \qquad (*)$$

Ya que c no aparece en ninguna fórmula del lado izquierdo, podemos aplicar el corolario 24G al segundo caso, y obtenemos

$$\Gamma \cup \{\theta_1, \ldots, \theta_m\} \vdash \forall x \, \varphi.$$

Esto y (*) contradicen la minimalidad de m (o la consistencia de Γ si $m = 0$).

Paso 3 : Ahora extendemos el conjunto consistente $\Gamma \cup \Theta$ a un conjunto consistente Δ que es maximal en el sentido de que para cualquier fórmula φ o bien $\varphi \in \Delta$ o $(\neg \varphi) \in \Delta$.

Detalles: podemos imitar la demostración utilizada en el argumento análogo de la demostración de compacidad para enunciados de la sección 7 del capítulo I, o bien podemos argumentar como sigue: Sea Λ el conjunto de axiomas lógicos para el lenguaje expandido. Como $\Gamma \cup \Theta$ es consistente, no existe fórmula β tal que $\Gamma \cup \Theta \cup \Lambda$ implique tautológicamente tanto β como $\neg \beta$. (Esto es por el teorema 24B, cuya demostración usa el teorema de compacidad de la lógica de enunciados.) Por lo tanto, hay una asignación de verdad v para el conjunto de todas las fórmulas primas que satisface a $\Gamma \cup \Theta \cup \Lambda$. Sea

$$\Delta = \{\varphi \mid \bar{v}(\varphi) = T\}.$$

Claramente, para cualquier φ, o $\varphi \in \Delta$ o $(\neg \varphi) \in \Delta$, pero no ambas. También tenemos que

$$\begin{aligned} \Delta \vdash \varphi &\Rightarrow \Delta \text{ implica tautológicamente } \varphi && \text{(ya que } \Lambda \subseteq \Delta\text{),} \\ &\Rightarrow \bar{v}(\varphi) = T && \text{ya que } v \text{ satisface } \Delta, \\ &\Rightarrow \varphi \in \Delta. \end{aligned}$$

En consecuencia, Δ es consistente, pues de otro modo tanto φ como $(\neg \varphi)$ pertenecerían a Δ.

En realidad, independientemente de cómo se haya construido Δ, debe ser deductivamente cerrado. Esto es,

$$\begin{aligned} \Delta \vdash \varphi &\Rightarrow \Delta \nvdash \neg \varphi && \text{por consistencia,} \\ &\Rightarrow (\neg \varphi) \notin \Delta, \\ &\Rightarrow \varphi \in \Delta && \text{por maximalidad.} \end{aligned}$$

Paso 4 Ahora, a partir de Δ construimos una estructura $\mathfrak{A}$ para el nuevo lenguaje, pero con el símbolo de igualdad (si lo hay) reemplazado por un nuevo símbolo de predicado E de dos argumentos. $\mathfrak{A}$ no será la estructura en la que Γ se satisfaga; será una estructura preliminar.

(a) $|\mathfrak{A}|$ = el conjunto de todos los términos del nuevo lenguaje.

(b) Definimos la relación binaria $E^{\mathfrak{A}}$ como

$$\langle u, t\rangle \in E^{\mathfrak{A}} \quad \text{sii la fórmula} \quad u = t \text{ pertenece a } \Delta.$$

(c) Para cada parámetro de predicado P de n argumentos, definimos la relación n-aria $P^{\mathfrak{A}}$ como

$$\langle t_1, \ldots, t_n\rangle \in P^{\mathfrak{A}} \quad \text{sii} \quad Pt_1 \cdots t_n \in \Delta.$$

(d) Para cada símbolo de función f de n argumentos, sea $f^{\mathfrak{A}}$ la función definida por

$$f^{\mathfrak{A}}(t_1, \ldots, t_n) = ft_1 \cdots t_n.$$

Esto incluye el caso $n = 0$; para un símbolo de constante c, tomamos $c^{\mathfrak{A}} = c$. También definimos una función $s : V \to |\mathfrak{A}|$, a saber, la función identidad $s(x) = x$ sobre V.

Entonces se sigue que para cualquier término t, $\bar{s}(t) = t$. Para cualquier fórmula φ, sea φ^* el resultado de reemplazar el símbolo de igualdad en φ por E. Entonces

$$\models_{\mathfrak{A}} \varphi^*[s] \quad \text{sii} \quad \varphi \in \Delta.$$

Detalles: Que $\bar{s}(t) = t$ puede probarse por inducción sobre t, pero la demostración es totalmente directa.

La otra afirmación, que

$$\models_{\mathfrak{A}} \varphi^*[s] \quad \text{sii} \quad \varphi \in \Delta,$$

la demostramos por inducción sobre el número de lugares en los que aparecen símbolos de conectivo o símbolos de cuantificador en φ.

Caso 1 Fórmulas atómicas. Hemos definido $\mathfrak{A}$ de manera tal que este caso sea inmediato. Por ejemplo, si φ es Pt, entonces

$$\begin{aligned} \models_{\mathfrak{A}} Pt[s] \quad &\text{sii} \quad \bar{s}(t) \in P^{\mathfrak{A}}, \\ &\text{sii} \quad t \in P^{\mathfrak{A}}, \\ &\text{sii} \quad Pt \in \Delta. \end{aligned}$$

De forma similar,

$$\begin{aligned} \models_{\mathfrak{A}} u\,E\,t[s] \quad &\text{sii} \quad (\bar{s}(u),\ \bar{s}(t)) \in E^{\mathfrak{A}}, \\ &\text{sii} \quad \langle u, t\rangle \in E^{\mathfrak{A}}, \\ &\text{sii} \quad u = t \in \Delta. \end{aligned}$$

Caso 2 Negación.

$$\begin{aligned} \models_{\mathfrak{A}} (\neg\varphi)^*[s] \ &\text{sii} \ \not\models_{\mathfrak{A}} \varphi^*[s], \\ &\text{sii} \ \varphi \notin \Delta \text{ por hipótesis inductiva}, \\ &\text{sii} \ (\neg\varphi) \in \Delta \text{ por las propiedades de } \Delta. \end{aligned}$$

Caso 3 Condicional.

$$\begin{aligned} \models_{\mathfrak{A}} (\varphi \to \psi)^*[s] \ &\text{sii} \ \not\models_{\mathfrak{A}} \varphi^*[s] \quad \text{o} \quad \models_{\mathfrak{A}} \psi^*[s], \\ &\text{sii} \ \varphi \notin \Delta \quad \text{o} \quad \psi \in \Delta \text{ por hipótesis inductiva}, \\ &\text{sii} \ (\neg\varphi) \in \Delta \quad \text{o} \quad \psi \in \Delta, \\ &\Rightarrow \Delta \vdash (\varphi \to \psi), \text{ de hecho tautológicamente}, \\ &\Rightarrow \varphi \notin \Delta \quad \text{o} \quad [\varphi \in \Delta \ \text{ y } \ \Delta \vdash \psi], \\ &\Rightarrow (\neg\varphi) \in \Delta \quad \text{o} \quad \psi \in \Delta, \end{aligned}$$

lo cual cierra el círculo. Y

$$\Delta \vdash (\varphi \to \psi) \quad \text{sii} \quad (\varphi \to \psi) \in \Delta.$$

(Esto debería compararse con el ejercicio 2 de la sección 7 del capítulo 1.)

Caso 4 Cuantificación. Queremos mostrar que

$$\models_{\mathfrak{A}} \forall x\, \varphi^*[s] \quad \text{sii} \quad \forall x\, \varphi \in \Delta.$$

(La ambigüedad de notación no causa riesgos, ya que $\forall x\,(\varphi^*)$ es lo mismo que $(\forall x\ \varphi)^*$). Δ incluye la fórmula θ:

$$\neg\forall x\,\varphi \to \neg\,\varphi^x_c.$$

Para mostrar que

$$\models_{\mathfrak{A}} \forall x\ \varphi^*[s] \Rightarrow \forall x\,\varphi \in \Delta,$$

podemos argumentar de la siguiente forma: si φ^* es verdadera para cualquier cosa, entonces es verdadera para c, de donde por hipótesis inductiva $\varphi^x_c \in \Delta$. Pero entonces $\forall x\ \varphi \in \Delta$,

porque c fue elegida como un contraejemplo para φ si es que había alguno. Con más detalle:

$\models_{\mathfrak{A}} \forall x\, \varphi^*[s] \Rightarrow\ \models_{\mathfrak{A}} \varphi^*[s(x \mid c)]$	
$\Rightarrow\ \models_{\mathfrak{A}} (\varphi^*)^x_c[s]$	por el lema de sustitución
$\Rightarrow\ \models_{\mathfrak{A}} (\varphi^x_c)^*[s],$	por ser la misma fórmula
$\Rightarrow \varphi^x_c \in \Delta$	por la hipótesis inductiva
$\Rightarrow (\neg \varphi^x_c) \notin \Delta$	por consistencia
$\Rightarrow (\neg \forall x\, \varphi) \notin \Delta$	ya que $\theta \in \Delta$ y Δ es deductivamente cerrado.
$\Rightarrow \forall x\, \varphi \in \Delta.$	

(Ésta es la única vez que usamos Θ. Necesitábamos saber que si $(\neg \forall x\, \varphi) \in \Delta$, entonces para una c particular tendríamos $(\neg \varphi^x_c) \in \Delta$.)

Ahora pasamos al inverso. Casi podemos argumentar como sigue:

$\not\models_{\mathfrak{A}} \forall x\, \varphi^*[s] \Rightarrow\ \not\models_{\mathfrak{A}} \varphi^*[s(x \mid t)]$	para algún término t
$\rightsquigarrow\ \not\models_{\mathfrak{A}} (\varphi^x_t)^*[s]$	por el lema de sustitución
$\Rightarrow \varphi^x_t \notin \Delta$	por la hipótesis inductiva
$\rightsquigarrow \forall x\, \varphi \notin \Delta$	ya que Δ es deductivamente cerrado.

En este caso, la falla radica en que las dos implicaciones onduladas requieren que t sea sustituible por x en φ. Es posible que esto sea falso, pero podemos utilizar la reparación usual: cambiamos φ por una variante alfabética ψ en la que t sea sustituible por x. Entonces

$\not\models_{\mathfrak{A}} \forall x\, \varphi^*[s] \Rightarrow\ \not\models_{\mathfrak{A}} \varphi^*[s(x \mid t)]$	para algún t, fijo de aquí en adelante
$\Rightarrow\ \not\models_{\mathfrak{A}} \psi^*[s(x \mid t)]$	por la equivalencia semántica de las variantes alfabéticas (Corolario 25D)
$\Rightarrow\ \not\models_{\mathfrak{A}} (\psi^x_t)^*[s]$	por el lema de sustitución
$\Rightarrow \psi^x_t \notin \Delta$	por la hipótesis inductiva
$\Rightarrow \forall x\, \psi \notin \Delta$	ya que Δ es deductivamente cerrado

$\Rightarrow \forall x\, \varphi \notin \Delta$ por la equivalencia sintáctica de las variantes alfabéticas (Teorema 24I).

Esto completa la lista de casos posibles; se sigue, por inducción, que para cualquier φ,

$$\models_{\mathfrak{A}} \varphi^{*}[s] \quad \text{sii} \quad \varphi \in \Delta.$$

Si nuestro lenguaje original no incluyó el símbolo de igualdad, entonces ya terminamos. Ya que únicamente necesitamos restringir $\mathfrak{A}$ al lenguaje original para obtener una estructura que satisfaga a cada elemento de Γ con la función identidad.

Pero ahora supongamos que el símbolo de igualdad está en el lenguaje. Entonces $\mathfrak{A}$ no servirá. Por ejemplo, si Γ contiene el enunciado $c = d$ (donde c y d son símbolos de constante distintos), entonces necesitamos una estructura $\mathfrak{B}$ en la cual $c^{\mathfrak{B}} = d^{\mathfrak{B}}$. Obtenemos $\mathfrak{B}$ como la estructura cociente $\mathfrak{A}/E$ de $\mathfrak{A}$ módulo $E^{\mathfrak{A}}$.

Paso 5 $E^{\mathfrak{A}}$ es una relación de equivalencia sobre $|\mathfrak{A}|$. Para cada t en $|\mathfrak{A}|$ sea $[t]$ su clase de equivalencia. $E^{\mathfrak{A}}$ es, de hecho, una *relación de congruencia* para $\mathfrak{A}$. Esto significa que se cumplen las condiciones siguientes:

(i) $E^{\mathfrak{A}}$ es una relación de equivalencia sobre $|\mathfrak{A}|$.

(ii) $P^{\mathfrak{A}}$ es compatible con $E^{\mathfrak{A}}$ para cada símbolo de predicado P:

$$\langle t_1, \ldots, t_n\rangle \in P^{\mathfrak{A}} \text{ y } t_i\, E^{\mathfrak{A}}\, t_i' \text{ para } 1 \leq i \leq n \Rightarrow \langle t_1', \ldots, t_n'\rangle \in P^{\mathfrak{A}}.$$

(iii) $f^{\mathfrak{A}}$ es compatible con $E^{\mathfrak{A}}$ para cada símbolo de función f:

$$t_i\, E^{\mathfrak{A}}\, t_i' \quad \text{para} \quad 1 \leq i \leq n \Rightarrow f^{\mathfrak{A}}(t_1, \ldots, t_n) E^{\mathfrak{A}}\, f^{\mathfrak{A}}(t_1', \ldots, t_n').$$

En estas circunstancias, podemos construir la estructura cociente $\mathfrak{A}/E$, definida como sigue:

(a) $|\mathfrak{A}/E|$ es el conjunto de todas las clases de equivalencia de elementos de $|\mathfrak{A}|$.

(b) Para cada símbolo de predicado P de n argumentos,

$$\langle [t_1], \ldots, [t_n] \rangle \in P^{\mathfrak{A}/E} \text{ sii } \langle t_1, \ldots, t_n \rangle \in P^{\mathfrak{A}}.$$

(c) Para cada símbolo de función f de n argumentos,

$$f^{\mathfrak{A}/E}([t_1], \ldots, [t_n]) = [f^{\mathfrak{A}}(t_1, \ldots, t_n)].$$

Esto incluye los casos $n = 0$:

$$c^{\mathfrak{A}/E} = [c^{\mathfrak{A}}].$$

Sea $h : |\mathfrak{A}| \to |\mathfrak{A}/E|$ la función natural:

$$h(t) = [t].$$

Entonces h es un homomorfismo de $\mathfrak{A}$ sobre $\mathfrak{A}/E$. Además, $E^{\mathfrak{A}/E}$ es la relación de igualdad sobre $|\mathfrak{A}/E|$. En consecuencia, para cualquier φ:

$$\begin{aligned} \varphi \in \Delta &\Leftrightarrow \models_{\mathfrak{A}} \varphi^*[s] \\ &\Leftrightarrow \models_{\mathfrak{A}/E} \varphi^*[h \circ s] \\ &\Leftrightarrow \models_{\mathfrak{A}/E} \varphi[h \circ s]. \end{aligned}$$

Así $\mathfrak{A}/E$ satisface todos los elementos de Δ (y, por lo tanto, todos los elementos de Γ) con $h \circ s$.

Detalles: Recordemos que

$$\begin{aligned} t\, E^{\mathfrak{A}} t' \quad &\text{sii} \quad (t = t') \in \Delta, \\ &\text{sii} \quad \Delta \vdash t = t'. \end{aligned}$$

(i) $E^{\mathfrak{A}}$ es una relación de equivalencia sobre $\mathfrak{A}$ por las propiedades de igualdad Ec1, Ec2 y Ec3.

(ii) $P^{\mathfrak{A}}$ es compatible con $E^{\mathfrak{A}}$ por la propiedad de igualdad Ec4.

(iii) $f^{\mathfrak{A}}$ es compatible con $E^{\mathfrak{A}}$ por la propiedad de igualdad Ec5.

Entonces de la compatibilidad de $P^{\mathfrak{A}}$ con $E^{\mathfrak{A}}$ se sigue que $P^{\mathfrak{A}/E}$ está bien definida. Igualmente, $f^{\mathfrak{A}/E}$ está bien definida porque $f^{\mathfrak{A}}$ es compatible con $E^{\mathfrak{A}}$.

Resulta inmediato a partir de la construcción que h es un homomorfismo de $\mathfrak{A}$ sobre $\mathfrak{A}/E$. Y

$$
\begin{aligned}
[t]\, E^{\mathfrak{A}/E}\, [t'] \quad &\text{sii} \quad t\, E^{\mathfrak{A}} t', \\
&\text{sii} \quad [t] = [t'].
\end{aligned}
$$

Finalmente,

$$
\begin{aligned}
\varphi \in \Delta &\Leftrightarrow \models_{\mathfrak{A}} \varphi^*[s] && \text{por el paso 4} \\
&\Leftrightarrow \models_{\mathfrak{A}/E} \varphi^*[h \circ s] && \text{por el teorema de homomorfismo} \\
&\Leftrightarrow \models_{\mathfrak{A}/E} \varphi[h \circ s],
\end{aligned}
$$

el último paso está justificado por el hecho de que $E^{\mathfrak{A}/E}$ es la relación de igualdad sobre $|\mathfrak{A}/E|$.

> Paso 6: Restrinja la estructura $\mathfrak{A}/E$ al lenguaje original. Esta restricción de $\mathfrak{A}/E$ satisface a todo elemento de Γ con $h \circ s$. ⊣

Para un lenguaje no numerable, es necesario hacer unas cuantas modificaciones a la demostración anterior del teorema de completud. Digamos que el lenguaje tiene cardinalidad λ. (Con esto queremos decir que tiene λ símbolos o, equivalentemente, λ fórmulas.) Describiremos las modificaciones necesarias, suponiendo que el lector tiene conocimiento sustancial de la teoría de conjuntos. En el paso 1 agregamos λ nuevos símbolos de constante; los detalles no cambian. En el paso 2, únicamente cambian los detalles. El cardinal λ es un ordinal inicial. (Implícitamente hemos bien ordenado el lenguaje.) "Numeremos" los pares

$$\langle \varphi_\alpha, x_\alpha \rangle_{\alpha < \lambda}$$

indexados por los ordinales menores que λ. Para $\alpha < \lambda$, θ_α es

$$\neg \forall x_\alpha \varphi_\alpha \rightarrow (\neg \varphi)^{x_\alpha}_{c_\alpha},$$

donde c_α es el primero de los nuevos símbolos de constante que no está en φ_α ni en θ_β para toda $\beta < \alpha$. (Esto excluye cuando mucho $\aleph_0 \cdot \text{card}(\alpha)$ símbolos de constante, así que quedan algunos.) Finalmente, en el paso 3, podemos obtener el conjunto maximal Δ usando el lema de Zorn. El resto de la demostración es igual.

Teorema de compacidad (a) Si $\Gamma \models \varphi$, entonces existe un subconjunto finito $\Gamma_0 \subseteq \Gamma$, tal que $\Gamma_0 \models \varphi$.

(b) Si cada subconjunto finito Γ_0 de Γ es satisfactible, entonces Γ es satisfactible.

En particular, un conjunto Σ de enunciados tiene un modelo sii cada subconjunto finito tiene un modelo.

Demostración Para probar la parte (a) del teorema de compacidad, simplemente observamos que

$$\begin{aligned} \Gamma \models \varphi &\Rightarrow \Gamma \vdash \varphi \\ &\Rightarrow \Gamma_0 \vdash \varphi \quad \text{para algún } \Gamma_0 \subseteq \Gamma \text{ finito, ya que las deducciones son finitas} \\ &\Rightarrow \Gamma_0 \models \varphi. \end{aligned}$$

La parte (b) tiene una demostración similar. Si cada subconjunto finito de Γ es satisfactible, entonces por correctud, cada subconjunto finito de Γ es consistente. Por lo tanto, Γ es consistente, ya que las deducciones son finitas. Así que, por completud, Γ es satisfactible. (De hecho, las partes (a) y (b) son equivalentes; véase el ejercicio 3 de la sección 7 del capítulo 1). ⊣

Cuando alguien oye hablar por primera vez del teorema de compacidad, su inclinación natural es intentar combinar (por medio de alguna operación algebraica o de teoría de conjuntos) las estructuras en las que se satisfacen los diferentes subconjuntos finitos, de manera tal que se obtenga una estructura en la que se satisfaga la totalidad del conjunto. De hecho, tal demostración *es* posible. La operación que se usa es la construcción del *ultraproducto*. Pero no haremos mayores comentarios acerca de esta atractiva posibilidad.

Nótese que en el teorema de compacidad intervienen únicamente nociones semánticas de la sección 2 de este capítulo; no

involucra para nada las deducciones; de hecho hay demostraciones que evitan las deducciones. Los mismos comentarios se aplican al teorema siguiente.

Teorema de numerabilidad En un lenguaje razonable, el conjunto de fórmulas válidas es efectivamente numerable.

Por lenguaje razonable entendemos un lenguaje cuyo conjunto de parámetros se puede numerar efectivamente y en el que las dos relaciones

$$\{\langle P, n\rangle \mid P \text{ es un símbolo de predicado de } n \text{ argumentos}\}$$

y

$$\{\langle f, n\rangle \mid f \text{ es un símbolo de función de } n \text{ argumentos}\}$$

son decidibles. Por ejemplo, cualquier lenguaje que tenga sólo una cantidad finita de parámetros (dicho lenguaje se llamará *lenguaje finito*) es ciertamente razonable, ya que los conjuntos finitos siempre son decidibles. Por otra parte, un lenguaje razonable deberá ser a lo más numerable, ya que no podemos numerar efectivamente un conjunto no numerable. (De hecho, cabe hacer una afirmación más fuerte: al igual que en la sección 7 del capítulo I, es necesario un formato adecuado de entrada/salida en el cual el conjunto subyacente de símbolos expresados sea *finito*, lo que implica que el conjunto de todas las cadenas es numerable.)

En la sección 4 del capítulo III, se dará una versión precisa de este teorema. (Véase especialmente ahí el inciso 20.) En esencia, las demostraciones de estas dos versiones son la misma.

Demostración El hecho esencial es que Λ es decidible, y por lo tanto el conjunto de deducciones es decidible.

Supongamos que se nos da cierta expresión ε. (La suposición de que el lenguaje es razonable ya está aquí. Sólo existe una cantidad numerable de cosas elegibles que una persona puede dar a otra.) Queremos decidir si ε está en Λ o no. Primero verificamos que ε tenga la forma sintáctica necesaria para ser una fórmula. (En

la lógica de enunciados dimos instrucciones detalladas para dicha verificación. Véase la sección 3 del capítulo l. Para lenguajes de primer orden se pueden dar instrucciones similares, utilizando la sección 3 de este capítulo). Si ε pasa esa prueba, entonces verificamos (construyendo una tabla de verdad) si es una generalización de una tautología. Si no, procedemos a ver si ε tiene la forma sintáctica necesaria para estar en el grupo 2 de axiomas. Y así sucesivamente. Si ε no ha sido aceptada cuando terminemos el grupo 6 de axiomas, entonces ε no está en Λ.

(Lo anterior pretende convencer al lector de que en verdad se puede distinguir entre los que son elementos de Λ y los que no lo son. El lector que aún tenga dudas puede buscar la segunda presentación en la sección 4 del capítulo III.)

Ya que Λ es decidible, el conjunto de consecuencias tautológicas de Λ es efectivamente numerable; véase el teorema 17G. Pero

$$\begin{aligned}&\{\alpha \mid \alpha \text{ es una consecuencia tautológica de } \Lambda\}\\ &\quad = \{\alpha \mid \vdash \alpha\} \quad \text{por el teorema 24B,}\\ &\quad = \{\alpha \mid \alpha \text{ es válida}\}. \qquad \dashv\end{aligned}$$

En el siguiente argumento se presenta una alternativa al párrafo anterior de esta prueba, que posiblemente arroje más luz: primero afirmamos que el conjunto de las deducciones (a partir de $\emptyset$) es decidible. Para una sucesión finita dada $\alpha_0, \ldots, \alpha_n$ podemos examinar cada α_i para ver si se encuentra en Λ o se puede obtener de elementos anteriores de la sucesión mediante modus ponens. Después, para numerar las fórmulas válidas, comenzamos por numerar todas las sucesiones finitas de fórmulas. Examinamos cada sucesión cuando aparece y decidimos si es o no una deducción. Si no lo es, la descartamos; pero si lo es, entonces ponemos su último elemento en la lista de fórmulas válidas. Continuando de esta manera, generamos —de una forma poco eficiente— una lista en la que a la larga aparecerá cualquier fórmula válida.

*Corolario 25F Sea Γ un conjunto decidible de fórmulas en un lenguaje razonable.

(a) El conjunto de teoremas de Γ es efectivamente numerable.

(b) El conjunto $\{\varphi \mid \Gamma \models \varphi\}$ de fórmulas implicadas lógicamente por Γ es efectivamente numerable.

(Por supuesto que las partes (a) y (b) se refieren al mismo conjunto. Este corolario incluye en sí mismo el teorema de numerabilidad, en el cual $\Gamma = \emptyset$.)

Demostración 1 Numeramos las fórmulas válidas; siempre que encontremos una de la forma

$$\alpha_n \to \cdots \to \alpha_1 \to \alpha_0,$$

verificamos si $\alpha_n, \ldots, \alpha_1$ se encuentran en Γ. Si es así, entonces ponemos α_0 en la lista de teoremas de Γ. De esta manera, finalmente se incluirá en la lista cualquier teorema de Γ. ⊣

Demostración 2 $\Gamma \cup \Lambda$ es decidible, así que su conjunto de consecuencias tautológicas es efectivamente numerable. Y éste es justamente el conjunto que queremos. ⊣

Por ejemplo, sea Γ el conjunto (decidible) de axiomas para cualquiera de los sistemas de teoría de conjuntos usuales. Entonces este corolario nos dice que el conjunto de teoremas de la teoría de conjuntos es efectivamente numerable.

De una manera más general, es natural insistir en que el conjunto de axiomas sea decidible al establecer alguna teoría axiomática. Después de todo, queremos que las demostraciones a partir de estos axiomas sean argumentos *convincentes* que puedan ser *verificados*. Parte del proceso de verificación supone revisar que los enunciados que se dice que son axiomas, sean de hecho axiomas. Para que esto sea posible, es necesario que el conjunto de axiomas sea decidible (o al menos semidecidible). Esto tiene como consecuencia que el conjunto de los teoremas que se siguen de los axiomas sea efectivamente numerable.

***Corolario 25G** Supongamos que Γ es un conjunto decidible de fórmulas en un lenguaje razonable, y que para cualquier enunciado σ, o bien $\Gamma \models \sigma$ o $\Gamma \models \neg\sigma$. Entonces el conjunto de enunciados que implica Γ es decidible.

Demostración Si Γ es inconsistente, entonces tendremos simplemente el conjunto (decidible) de todos los enunciados. Así que supongamos que Γ es consistente. Supongamos que se nos da un enunciado σ y se nos pide que decidamos si $\Gamma \models \sigma$ o no. Podemos numerar los teoremas de Γ y buscar σ o $\neg\sigma$. Finalmente aparecerá alguno y así sabremos la respuesta. ⊣

(Nótese que esta demostración realmente describe dos procedimientos de decisión. Uno es correcto cuando Γ es inconsistente, y el otro es correcto cuando Γ es consistente. Así que existe un procedimiento de decisión para cada caso. Pero no necesariamente podremos determinar efectivamente, dada una descripción finita de Γ, cuál deberá usarse. Un conjunto es decidible si *existe* un procedimiento de decisión para él, y esto no es lo mismo que tener en nuestras manos un procedimiento conocido de decisión.)

Debemos observar que, en general, nuestras demostraciones de numerabilidad no pueden convertirse en demostraciones de decidibilidad. Casi para todos los lenguajes, el conjunto de fórmulas válidas *no* es decidible. (Véase el teorema de Church, sección 5 del capítulo III.)

Notas históricas

El teorema de completud (para lenguajes numerables) se encuentra en la disertación doctoral de Kurt Gödel de 1930. (No debe confundirse con el "teorema de incompletud de Gödel", publicado en 1931; abordaremos este último resultado en el capítulo III.) El teorema de compacidad (para lenguajes numerables) se dio como un corolario.

El teorema de compacidad para lenguajes no numerables estaba implícito en un artículo de 1936 de Anatolii Mal'cev. Su demostración usaba funciones de Skolem (véase la sección 2 del capítulo IV) y el teorema de compacidad para la lógica de enunciados. La primera formulación explícita del teorema de

compacidad para lenguajes no numerables se encuentra en un artículo de Mal'cev de 1941.

Tanto el teorema de numerabilidad, como lo que se sigue del trabajo de Gödel de 1930, estaba implícito en los resultados publicados por Thoralf Skolem en 1928.

La demostración que hemos ofrecido del teorema de completud está basada en la que hizo Leon Henkin en su tesis, publicada en 1949. A diferencia de la prueba original de Gödel, la prueba de Henkin se generaliza fácilmente a lenguajes de cualquier cardinalidad.

Ejercicios

1. (Regla semántica IE) Supongamos que el símbolo de constante c no ocurre en φ ni en ψ ni en Γ, y que $\Gamma;\ \varphi^x_c \models \psi$. Muestre (sin utilizar los teoremas de correctud y de completud) que $\Gamma;\ \exists x\, \varphi \models \psi$.

2. Demuestre la equivalencia de las partes (a) y (b) del teorema de completud. *Sugerencia:* $\Gamma \models \varphi$ sii $\Gamma \cup \{\neg \varphi\}$ es insatisfactible. Y Δ es satisfactible sii $\Delta \not\models \bot$, donde $\bot$ es alguna fórmula refutable insatisfactible, tal como $\neg \forall x\, x = x$.

   Observación: De manera similar, el teorema de correctud es equivalente a la afirmación de que todo conjunto de fórmulas que es satisfactible es consistente.

3. Suponga que $\Gamma \vdash \varphi$ y que P es un símbolo de predicado que no ocurre ni en Γ ni en φ. ¿Hay una deducción de φ a partir de Γ en la que P no ocurra? *Sugerencia:* Hay dos enfoques muy diferentes para abordar este problema. El enfoque "suave" hace uso de dos lenguajes, uno que contiene a P y otro que no lo contiene. La aproximación "dura" considera la posibilidad de eliminar sistemáticamente P de una deducción dada de φ a partir de Γ.

4. Sea $\Gamma = \{\neg \forall v_1\, Pv_1, Pv_2, Pv_3, \ldots\}$. ¿Es Γ consistente? ¿Es Γ satisfactible?

5. Muestre que un mapa infinito puede ser coloreado con cuatro colores sii cada uno de los submapas de éste puede ser coloreado con cuatro colores. *Sugerencia:* Tome un

lenguaje que tenga símbolos de constante para cada país y que tenga cuatro símbolos de predicado de un argumento para los colores. Utilice el teorema de compacidad.

6. Sean Σ_1 y Σ_2 conjuntos de enunciados tales que no hay un modelo de ambos Σ_1 y Σ_2. Muestre que hay un enunciado τ tal que $\text{Mod}\,\Sigma_1 \subseteq \text{Mod}\,\tau$ y $\text{Mod}\,\Sigma_2 \subseteq \text{Mod}\,\neg\tau$. (Esto se puede expresar así: las clases disjuntas EC_Δ pueden separarse por una clase EC.) *Sugerencia:* $\Sigma_1 \cup \Sigma_2$ no es satisfactible; aplique compacidad.

7. El teorema de completud nos dice que cada enunciado cuenta con una deducción (a partir de $\emptyset$) o con un contramodelo (es decir, una estructura en la que es falso). Para cada uno de los enunciados siguientes, muestre que hay una deducción o dé un contramodelo.

   (a) $\forall x\,(Qx \to \forall y\, Qy)$

   (b) $(\exists x\, Px \to \forall y\, Qy) \to \forall z\,(Pz \to Qz)$

   (c) $\forall z\,(Pz \to Qz) \to (\exists x\, Px \to \forall y\, Qy)$

   (d) $\neg\exists y\,\forall x\,(Pxy \leftrightarrow \neg Pxx)$

8. Suponga el lenguaje (con igualdad) que tiene únicamente los parámetros $\forall$ y P, donde P es un símbolo de predicado de dos argumentos. Sea $\mathfrak{A}$ la estructura con $|\mathfrak{A}| = \mathbb{Z}$ el conjunto de los enteros (positivos, negativos y cero) y con $\langle a, b\rangle \in P^{\mathfrak{A}}$ sii $|a - b| = 1$. Por lo tanto, $\mathfrak{A}$ se ve como una gráfica infinita:

$$\cdots \longleftrightarrow \bullet \longleftrightarrow \bullet \longleftrightarrow \bullet \longleftrightarrow \cdots$$

   Muestre que hay una estructura elementalmente equivalente $\mathfrak{B}$ que no es conexa. (Ser *conexa* significa que para cada dos elementos de $|\mathfrak{B}|$, hay una trayectoria entre ellos. Una *trayectoria*, de longitud n, de a a b es una sucesión $\langle p_0, p_1, \ldots, p_n\rangle$ con $a = p_0$, $b = p_n$ y $\langle p_i, p_{i+1}\rangle \in P^{\mathfrak{B}}$ para cada i.) *Sugerencia:* Agregue los símbolos de constante c y d. Escriba enunciados que digan que c y d se encuentran alejados. Aplique compacidad.

9. En la sección 4 de este capítulo utilizamos cierto conjunto Λ de axiomas lógicos. Dentro de ciertos límites, ese conjunto puede ser modificado.
   (a) Suponga que agregamos a Λ una fórmula ψ que no es válida. Muestre que en ese caso falla el teorema de correctud.
   (b) En el otro extremo, suponga que no tomamos ningún axioma lógico: $\Lambda = \emptyset$. Muestre que en ese caso falla el teorema de completud.
   (c) Suponga que modificamos Λ agregando una nueva fórmula válida. Explique por qué se siguen cumpliendo tanto el teorema de correctud como el de completud.

6. *Modelos de teorías*

En esta sección dejaremos de lado las deducciones y los axiomas lógicos, y volveremos a los temas abordados en la sección 2 de este capítulo. Sin embargo, con base en los teoremas de la sección previa, ahora será posible responder más preguntas de las que podíamos responder anteriormente.

Modelos finitos

Algunos enunciados tienen únicamente modelos infinitos; por ejemplo, el enunciado que dice que $<$ es un orden sin elemento máximo. La negación de dicho enunciado es *finitamente válida*, esto es, es verdadera en toda estructura finita.

También es posible tener enunciados que tengan únicamente modelos finitos. Por ejemplo, cualquier modelo de $\forall x\ \forall y\ x = y$ tiene cardinalidad 1. Pero si todos los modelos de Σ son finitos, entonces el tamaño de sus modelos tiene una cota finita, como lo establece el siguiente teorema:

Teorema 26A Si un conjunto Σ tiene modelos finitos arbitrariamente grandes, entonces tiene un modelo infinito.

Demostración Para cada entero positivo $k \geq 2$, podemos encontrar un enunciado λ_k que se traduce: "Hay al menos k objetos." Por ejemplo,

$$\lambda_2 = \exists v_1 \, \exists v_2 \, v_1 \neq v_2,$$
$$\lambda_3 = \exists v_1 \, \exists v_2 \, \exists v_3 \, (v_1 \neq v_2 \land v_1 \neq v_3 \land v_2 \neq v_3).$$

Considere el conjunto

$$\Sigma \cup \{\lambda_2, \lambda_3, \ldots\}.$$

Por hipótesis, cualquier subconjunto finito tiene un modelo; así que, por compacidad, todo el conjunto tiene un modelo, que evidentemente tiene que ser infinito. ⊣

Por ejemplo, *a priori* es posible pensar que existe una ecuación sofisticada de la teoría de grupos que sea verdadera en todo grupo finito, pero falsa en todo grupo infinito. Sin embargo, de acuerdo con el teorema anterior, dicha ecuación no existe.

La demostración de este teorema ilustra un método útil para obtener una estructura con propiedades dadas. Escribimos enunciados (posiblemente en un lenguaje expandido) que establecen las propiedades que queremos. Después argumentamos que cualquier subconjunto finito de estos enunciados tiene un modelo. El teorema de compacidad hace el resto. En las páginas que siguen veremos más ejemplos de este método.

Corolario 26B La clase de todas las estructuras finitas (para un lenguaje fijo) no es EC_Δ. La clase de todas las estructuras infinitas no es EC.

Demostración El primer enunciado se sigue inmediatamente del teorema. Si la clase de todas las estructuras infinitas es $\text{Mod}\,\tau$, entonces la clase de todas las estructuras finitas es $\text{Mod}\,\neg\tau$. Pero esta clase ni siquiera se encuentra en EC_Δ, mucho menos en EC. ⊣

La clase de las estructuras infinitas *es* EC_Δ, siendo $\text{Mod}\{\lambda_2, \lambda_3, \ldots\}$.

A continuación queremos considerar problemas de decisión relacionados con estructuras finitas. Para cualquier estructura $\mathfrak{A}$, definimos la *teoría* de $\mathfrak{A}$, denotada por $\text{Th}\,\mathfrak{A}$, como el conjunto de todos los enunciados verdaderos en $\mathfrak{A}$. Dada una estructura *finita* $\mathfrak{A}$, nos preguntamos si el conjunto $\text{Th}\,\mathfrak{A}$ es decidible, y lo mismo para el conjunto de enunciados que tienen modelos finitos.

Las siguientes observaciones ayudarán a dar una respuesta:

1. Toda estructura finita $\mathfrak{A}$ es isomorfa a una estructura con universo $\{1, 2, \ldots, n\}$, donde n es el tamaño de $\mathfrak{A}$ (es decir, $n = \text{card } |\mathfrak{A}|$). La idea es que si $|\mathfrak{A}| = \{a_1, \ldots, a_n\}$, entonces se reemplace a_i por i.

Por ejemplo, supongamos que el lenguaje tiene únicamente el parámetro $\forall$ y un símbolo de predicado E de dos argumentos (para la relación de "arista" en una gráfica dirigida). Considere la estructura finita $\mathfrak{B}$ con universo $|\mathfrak{B}|$, compuesta por un conjunto de cuatro objetos distintos $\{a, b, c, d\}$, y con

$$E^{\mathfrak{B}} = \{\langle a, b\rangle, \langle b, a\rangle, \langle b, c\rangle, \langle c, c\rangle\}.$$

Entonces $\mathfrak{B}$ es isomorfa a la estructura

$$(\{1, 2, 3, 4\}; \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 3\rangle, \langle 3, 3\rangle\}).$$

Sin embargo, para este caso existen otras posibilidades; si nos hubiéramos centrado en los elementos de $|\mathfrak{B}|$ ordenados como b, a, d, c, tendríamos una estructura isomorfa, aunque diferente:

$$(\{1, 2, 3, 4\}; \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 1, 4\rangle, \langle 4, 4\rangle\}).$$

2. Una estructura finita del tipo que acabamos de describir puede describirse, para un lenguaje finito, mediante una cadena finita de símbolos. En el ejemplo,

$$(\{1, 2, 3, 4\}; \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 3\rangle, \langle 3, 3\rangle\}),$$

esta línea describe completamente la estructura y se puede escribir con numerales en base 10 (o en su base favorita) junto con puntuación y delimitadores (por ejemplo, paréntesis). Por lo tanto, dicha estructura puede ser *comunicada* a otra persona o a una máquina. La cadena finita de símbolos puede escribirse en un formato adecuado de entrada.

3. Dada una estructura finita $\mathfrak{A}$ para un lenguaje finito, con universo $\{1, \ldots, n\}$ (y, por la observación anterior, sabemos que dicho objeto *puede ser* dado), una fórmula φ y una asignación s_φ de números de este universo a las variables libres

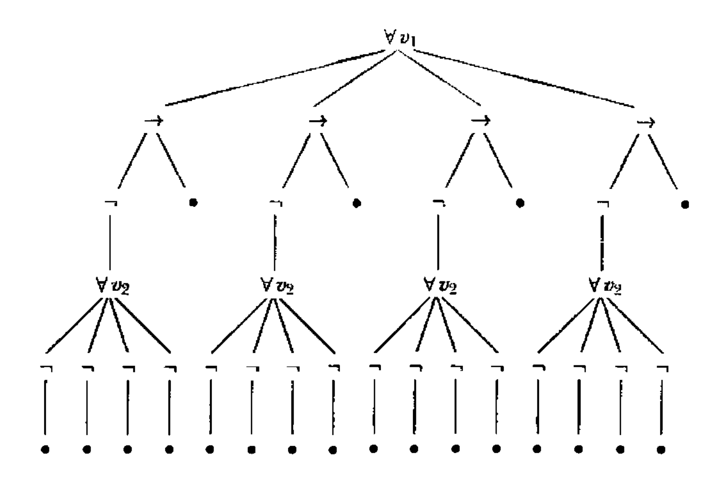


FIGURA 9. *Revisión del enunciado* $\forall v_1\ ((\neg\forall v_2\ \neg E\ v_2\, v_1) \rightarrow E\ v_1\, v_1)$ *en una estructura con universo de tamaño 4.*

de φ (por supuesto que sólo hay una cantidad finita), podemos determinar efectivamente si $\models_{\mathfrak{A}} \varphi[s_\varphi]$ o no.

Por ejemplo, dada

$$\mathcal{B} = (\{1, 2, 3, 4\}; \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 3\rangle, \langle 3, 3\rangle\}).$$
$$\varphi = \forall v_1\ ((\neg\forall v_2\ \neg\, E\ v_2\, v_1) \rightarrow E\ v_1\ v_1),$$

podemos organizar la computación en la forma del árbol que aparece en la figura 9. Vemos que el enunciado φ, que dice "Cualquier cosa en el rango de E está relacionada consigo misma", es falso en $\mathfrak{B}$.

En cada hoja del árbol (es decir, en cada vértice minimal) tenemos una fórmula atómica, así que damos una "ojeada a la tabla" para ver si esto se satisface. Nótese que todo cuantificador genera una búsqueda a través del universo de n elementos. Dada una fórmula φ con k cuantificadores, el número de hojas del árbol está acotado por un polinomio de grado k en términos de n. Si el lenguaje contiene símbolos de función, entonces

es necesario evaluar cada término utilizando la función (finita) que ofrece la estructura.

En particular, al restringirnos a los enunciados, podemos, dada $\mathfrak{A}$ como antes y un enunciado σ, decidir efectivamente si $\mathfrak{A}$ es un modelo de σ o no. (De hecho, σ podría ser aquí un enunciado de segundo orden, como en el capítulo IV.)

***Teorema 26C** Si $\mathfrak{A}$ es una estructura finita en un lenguaje finito, entonces $\text{Th}\,\mathfrak{A}$ es decidible.

Demostración 1 Por la observación 1, podemos reemplazar $\mathfrak{A}$ por una estructura isomorfa con un universo de la forma $\{1, \ldots, n\}$, sin que cambie cuáles son los enunciados verdaderos. Después, apliquemos la observación 3. ⊣

Demostración 2 Por el ejercicio 17 (a) de la sección 2 de este capítulo, hay un enunciado $\delta_{\mathfrak{A}}$ que caracteriza $\mathfrak{A}$, salvo isomorfismo. De donde se sigue que:

$$\text{Th}\,\mathfrak{A} = \{\sigma \mid \delta_{\mathfrak{A}} \models \sigma\}.$$

(Detalles: para demostrar "$\subseteq$" nótese que si σ es verdadero en $\mathfrak{A}$, entonces es verdadero en todas las copias isomorfas y, por lo tanto, en todos los modelos de $\delta_{\mathfrak{A}}$. De modo que $\delta_{\mathfrak{A}} \models \sigma$. En la otra dirección, la demostración es más sencilla; si $\delta_{\mathfrak{A}} \models \sigma$, entonces σ es verdadero en todos los modelos de $\delta_{\mathfrak{A}}$, uno de los cuales es $\mathfrak{A}$.) Aplique el corolario 25G, notando que para todo σ, o bien $\models_{\mathfrak{A}} \sigma$ o $\models_{\mathfrak{A}} \neg\sigma$. ⊣

4. Dado un enunciado σ y un entero positivo n, podemos decidir efectivamente si σ tiene o no un modelo con n elementos. Es decir, que la relación binaria

$$\{\langle \sigma, n \rangle \mid \sigma \text{ tiene un modelo de tamaño } n\}$$

es decidible.

La idea clave es que solamente hay que revisar una cantidad finita de estructuras, cosa que ciertamente podemos hacer. Por la observación 1, el enunciado σ tiene un modelo de tamaño n si y sólo si tiene un modelo con universo $\{1, \ldots, n\}$. Si restringimos el lenguaje a los parámetros que ocurren en σ, solamente

hay una cantidad finita de ese tipo de estructuras y podemos generarlas todas sistemáticamente. (Por ejemplo, si los únicos parámetros son $\forall$ y un símbolo de predicado de dos argumentos, entonces habrá 2^{n^2} estructuras diferentes.) Usando la observación 3, verificamos si alguna de éstas es modelo de σ.

5. El *espectro* de un enunciado σ se define como $\{n \mid \sigma$ tiene un modelo de tamaño $n\}$. Vea el ejercicio 16 de la sección 2 de este capítulo (p. 151). De la observación 4 se sigue que el espectro de cualquier enunciado es un conjunto decidible de enteros positivos.

***Teorema 26D** Para un lenguaje finito, $\{\sigma \mid \sigma$ tiene un modelo finito$\}$ es efectivamente numerable.

Demostración A continuación damos un procedimiento de semidecisión: dado σ, usando la observación 4, revise primero si éste tiene un modelo de tamaño 1; si no lo tiene, inténtelo con 2, y así sucesivamente. ⊣

***Corolario 26E** Supongamos que el lenguaje es finito y sea Φ el conjunto de enunciados verdaderos en toda estructura *finita*. Entonces su complemento $\overline{\Phi}$ es efectivamente numerable.

Demostración Dado un enunciado σ,

$$\sigma \in \overline{\Phi} \iff (\neg\sigma) \text{ tiene un modelo finito.}$$

Podemos aplicar el procedimiento anterior de semidecisión a $(\neg\sigma)$. ⊣

Se sigue (por el teorema 17F) que Φ es decidible si y sólo si es efectivamente numerable. Pero esto no sucede. Entonces, sin dar la demostración, afirmamos el siguiente:

***Teorema de Trakhtenbrot (1950)** El conjunto de enunciados

$$\Phi = \{\sigma \mid \sigma \text{ es verdadero en toda estructura finita}\}$$

no es en general decidible ni efectivamente numerable.

Así que el análogo del teorema de numerabilidad restringido a estructuras finitas es falso.

Tamaño de modelos

En la prueba del teorema de completud que aparece en la sección 5 de este capítulo, comenzamos con un conjunto consistente Γ y construimos una estructura $\mathfrak{A}/E$ en la que se satisfacía el conjunto. ¿Qué tan grande era esa estructura? Afirmamos que si nuestro lenguaje inicial es numerable, entonces $|\mathfrak{A}/E|$ es un conjunto numerable. De modo que un conjunto consistente de enunciados en un lenguaje numerable tiene un modelo numerable.

$\mathfrak{A}/E$ se construyó a partir de una estructura preliminar $\mathfrak{A}$. El universo de $\mathfrak{A}$ era el conjunto de todos los términos del lenguaje obtenido al agregar un conjunto numerable de nuevos símbolos de constante. Sin embargo, el lenguaje aumentado seguía siendo numerable, así que el conjunto de todas las expresiones (y, por ello, el conjunto de todos los términos) era numerable. Es decir, $|\mathfrak{A}|$ era numerable.

El universo de $\mathfrak{A}/E$ estaba compuesto por las clases de equivalencia de elementos de $\mathfrak{A}$, así que éste también era un conjunto numerable. (Podemos dar una función inyectiva de $|\mathfrak{A}/E|$ en $|\mathfrak{A}|$ si a cada clase de equivalencia se le asigna un elemento representante.) La conclusión es que, tal como se afirmaba, $\mathfrak{A}/E$ es una estructura numerable.

Teorema de Löwenheim-Skolem (1915) (a) Sea Γ un conjunto satisfactible de fórmulas en un lenguaje numerable. Entonces hay una estructura numerable que satisface Γ.

(b) Sea Σ un conjunto de enunciados en un lenguaje numerable. Si Σ tiene un modelo, entonces tiene un modelo numerable.

Demostración Primero, obsérvese que Γ es consistente, por el teorema de correctud. Entonces, por el teorema de completud (junto con las observaciones que hemos hecho hasta ahora), hay una estructura numerable que lo satisface. $\dashv$

(Hay otra demostración más directa de este teorema que se dará en la sección 2 del capítulo IV; préstese especial atención al ejercicio 1 de dicha sección. Esa prueba, que no usa un cálculo deductivo, comienza con una estructura arbitra-

ria $\mathfrak{A}$ que satisface Γ, y mediante diversas manipulaciones se extrae de ella una *subestructura* numerable que todavía satisface Γ.)

El teorema de Löwenheim-Skolem fue publicado por Leopold Löwenheim en 1915 para el caso en el que Γ es un conjunto unitario; en 1920, Thoralf Skolem lo generalizó a un Γ posiblemente infinito. El teorema marcó una nueva fase en la lógica matemática. El trabajo anterior se había encaminado a *formalizar* las matemáticas por medio de lenguajes formales y cálculos deductivos; el inicio de este trabajo en 1879 se debe en gran parte a Gottlob Frege. Por ejemplo, en los *Principia Mathematica* (1910–1913) de Whitehead y Russell se realizó dicha formalización con sumo detalle. Sin embargo, el periodo moderno empezó cuando los lógicos dieron un paso atrás y comenzaron a probar resultados acerca de los sistemas formales que se habían estado construyendo. David Hilbert, Emil Post, Kurt Gödel (ya mencionado) y Alfred Tarski, entre otros, realizaron trabajos en esa dirección.

Para dar un ejemplo de la aplicación del teorema de Löwenheim-Skolem: sea A_{ST} el conjunto de axiomas que el lector prefiera de la teoría de conjuntos. Obviamente, presuponemos que esos axiomas son consistentes y, por lo tanto, que tienen un modelo. Por el teorema de Löwenheim-Skolem, esos axiomas tienen un modelo numerable $\mathfrak{S}$. Por supuesto, $\mathfrak{S}$ también es modelo de todos los enunciados implicados lógicamente por A_{ST}. Uno de estos enunciados afirma (cuando se traduce al español, mediante la traducción propuesta) que hay una cantidad no numerable de conjuntos. Aquí no hay contradicción, pero la situación es lo suficientemente desconcertante como para que se la llame "la paradoja de Skolem". Lo que es cierto *en la estructura* $\mathfrak{S}$ es que no hay ningún elemento que satisfaga la definición formal de ser una función biyectiva de los números naturales en el universo. Pero esto de ninguna manera excluye la posibilidad de que haya (fuera de $\mathfrak{S}$) una auténtica función que nos dé esa correspondencia uno a uno.

Recuerde que la *teoría* de $\mathfrak{A}$, denotada por Th $\mathfrak{A}$, es el conjunto de todos los enunciados verdaderos en $\mathfrak{A}$. Podemos aplicar el teorema de Löwenheim-Skolem (con $\Sigma = \text{Th}\,\mathfrak{A}$) para probar que para cualquier estructura $\mathfrak{A}$ de un lenguaje numerable,

existe una estructura *numerable* $\mathfrak{B}$ elementalmente equivalente a ella. Si $\mathfrak{B}$ es un modelo de $\mathrm{Th}\,\mathfrak{A}$, entonces $\mathfrak{A} \equiv \mathfrak{B}$, pues

$$\models_{\mathfrak{A}} \sigma \Rightarrow \sigma \in \mathrm{Th}\,\mathfrak{A} \Rightarrow \models_{\mathfrak{B}} \sigma$$

y

$$\not\models_{\mathfrak{A}} \sigma \Rightarrow \models_{\mathfrak{A}} \neg\sigma \Rightarrow (\neg\sigma) \in \mathrm{Th}\,\mathfrak{A} \Rightarrow \models_{\mathfrak{B}} \neg\sigma \Rightarrow \not\models_{\mathfrak{B}} \sigma.$$

Por ejemplo, el campo de los reales $(\mathbb{R}; 0, 1, +, \cdot)$ es una estructura no numerable para un lenguaje finito. Por lo tanto, deberá existir alguna estructura numerable (también un campo) que satisfaga exactamente los mismos enunciados. (De hecho, Tarski demostró que podemos tomar el campo de los números reales algebraicos.)

Ejemplo Considere la estructura

$$\mathfrak{N} = (\mathbb{N}; 0, S, <, +, \cdot).$$

Afirmamos que existe una estructura numerable $\mathfrak{M}_0$, elementalmente equivalente a $\mathfrak{N}$ (es decir, $\mathfrak{M}_0$ y $\mathfrak{N}$ satisfacen exactamente los mismos enunciados), pero que no es isomorfa a $\mathfrak{N}$.

Demostración Construiremos $\mathfrak{M}_0$ usando el teorema de compacidad. Extendamos el lenguaje agregando un nuevo símbolo de constante c. Sea

$$\Sigma = \{\mathbf{0} < c, \mathbf{S0} < c, \mathbf{SS0} < c, \ldots\}.$$

Afirmamos que $\Sigma \cup \mathrm{Th}\,\mathfrak{N}$ tiene un modelo. Para demostrarlo, tómese cualquier subconjunto finito de $\Sigma \cup \mathrm{Th}\,\mathfrak{N}$. Ese subconjunto finito es verdadero en

$$\mathfrak{N}_k = (\mathbb{N}; 0, S, <, +, \cdot, k)$$

(donde $k = c^{\mathfrak{N}_k}$) para alguna k suficientemente grande. De modo que, por el teorema de compacidad, $\Sigma \cup \mathrm{Th}\,\mathfrak{N}$ tiene un modelo.

Usando el teorema de Löwenheim-Skolem, $\Sigma \cup \mathrm{Th}\,\mathfrak{N}$ tiene un modelo numerable

$$\mathfrak{M} = (|\mathfrak{M}|; \mathbf{0}^{\mathfrak{M}}, \mathbf{S}^{\mathfrak{M}}, <^{\mathfrak{M}}, +^{\mathfrak{M}}, \cdot^{\mathfrak{M}}, c^{\mathfrak{M}}).$$

Sea $\mathfrak{M}_0$ la restricción de $\mathfrak{M}$ al lenguaje original:

$$\mathfrak{M}_0 = (|\mathfrak{M}|; 0^{\mathfrak{M}}, S^{\mathfrak{M}}, <^{\mathfrak{M}}, +^{\mathfrak{M}}, \cdot^{\mathfrak{M}}).$$

Como $\mathfrak{M}_0$ es modelo de $\text{Th}\,\mathfrak{N}$, tenemos que $\mathfrak{M}_0 \equiv \mathfrak{N}$:

$$\models_{\mathfrak{N}} \sigma \Rightarrow \sigma \in \text{Th}\,\mathfrak{N} \Rightarrow \models_{\mathfrak{M}_0} \sigma$$
$$\not\models_{\mathfrak{N}} \sigma \Rightarrow \neg\sigma \in \text{Th}\,\mathfrak{N} \Rightarrow \models_{\mathfrak{M}_0} \neg\sigma \Rightarrow \not\models_{\mathfrak{M}_0} \sigma.$$

Dejamos al lector la tarea de verificar que $\mathfrak{M}_0$ no es isomorfo a $\mathfrak{N}$. ($|\mathfrak{M}_0|$ contiene el número "infinito" $c^{\mathfrak{M}}$.) ⊣

¿Qué sucede con los lenguajes no numerables?[4] Supongamos que en la demostración del teorema de completud comenzamos con un conjunto Γ en un lenguaje de cardinalidad λ. Afirmamos que, en este caso, la estructura $\mathfrak{A}/E$ que construimos tiene cardinalidad $\leq \lambda$.

$\mathfrak{A}/E$ se construyó a partir de la estructura preliminar $\mathfrak{A}$. El universo de $\mathfrak{A}$ era el conjunto de todos los términos en un lenguaje que se obtuvo al agregar λ nuevos símbolos de constante. Así que el lenguaje aumentado aún tenía cardinalidad λ. Así, (por el teorema 0D) el conjunto de todas las expresiones (y por lo tanto, el conjunto de todos los términos) tenía cardinalidad $\leq \lambda$. (De hecho, puesto que al menos teníamos los λ nuevos símbolos de constante, el conjunto de términos tenía exactamente cardinalidad λ.)

El universo de $\mathfrak{A}/E$ estaba compuesto por clases de equivalencia de elementos de $\mathfrak{A}$, así que card $|\mathfrak{A}/E| \leq$ card $|\mathfrak{A}|$. (Podríamos dar una función inyectiva de $|\mathfrak{A}/E|$ en $|\mathfrak{A}|$, al asignar a cada clase de equivalencia alguno de sus elementos, pero es posible que para eso se necesite el axioma de elección.) Así, una vez aclarada la cuestión, se ve que Γ se satisface en una estructura $\mathfrak{A}/E$ de cardinalidad $\leq \lambda$.

Teorema de Löwenheim-Skolem (a) Sea Γ un conjunto satisfactible de fórmulas en un lenguaje de cardinalidad λ. Entonces Γ es satisfactible en alguna estructura de tamaño $\leq \lambda$.

[4] Se sugiere al lector que desee evitar los cardinales no numerables, pasar a la subsección "Teorías".

(b) Sea Σ un conjunto de enunciados de un lenguaje de cardinalidad λ. Si Σ tiene un modelo, entonces tiene un modelo de cardinalidad $\leq \lambda$.

La primera versión del teorema de Löwenheim-Skolem que presentamos es un caso particular de esta versión, en la que $\lambda = \aleph_0$.

Supongamos que tenemos una estructura no numerable $\mathfrak{A}$ para un lenguaje numerable. Por el teorema de Löwenheim-Skolem (aplicado a Th $\mathfrak{A}$) hay una estructura $\mathfrak{B}$ numerable que es modelo de Th $\mathfrak{A}$, por lo que $\mathfrak{A} \equiv \mathfrak{B}$, como ya se hizo notar antes.

De manera inversa, supongamos que comenzamos con una estructura finita o numerable $\mathfrak{B}$. ¿Existe una estructura $\mathfrak{A}$ no numerable tal que $\mathfrak{A} \equiv \mathfrak{B}$? Si $\mathfrak{B}$ es finita (y el lenguaje incluye la igualdad), entonces esto es imposible. Pero si $\mathfrak{B}$ es infinita, entonces sí habrá tal $\mathfrak{A}$, gracias al siguiente "teorema ascendente y descendente de Löwenheim-Skolem". La parte ascendente se debe a Tarski, y de ahí la "T" de "LST".

Teorema LST Sea Γ un conjunto de fórmulas en un lenguaje de cardinalidad λ, y supongamos que Γ es satisfactible en alguna estructura infinita. Entonces, para todo cardinal $\kappa \geq \lambda$, hay una estructura de cardinalidad κ en la que Γ es satisfactible.

Demostración Sea $\mathfrak{A}$ la estructura infinita en la que Γ es satisfactible. Extendemos el lenguaje agregando un conjunto C de κ nuevos símbolos de constante. Sea

$$\Sigma = \{c_1 \neq c_2 \mid c_1, c_2 \text{ elementos distintos de } C\}.$$

Entonces, cada subconjunto finito de $\Sigma \cup \Gamma$ es satisfactible en la estructura $\mathfrak{A}$, extendida para asignar objetos distintos a la cantidad finita de nuevos símbolos de constante del subconjunto. (Como $\mathfrak{A}$ es infinito, hay elementos suficientes para dar cabida a cualquier número finito de ellos.) Así que, por compacidad, $\Sigma \cup \Gamma$ es satisfactible, y por el teorema de Löwenheim-Skolem puede ser satisfecho en una estructura $\mathfrak{B}$ de cardinalidad $\leq \kappa$. (El lenguaje expandido tiene cardinalidad $\lambda + \kappa = \kappa$.) Pero

es evidente que cualquier modelo de Σ tiene cardinalidad $\geq \kappa$. Así que $\mathfrak{B}$ tiene cardinalidad κ; finalmente restringimos $\mathfrak{B}$ al lenguaje original. ⊣

Corolario 26F (a) Sea Σ un conjunto de enunciados en un lenguaje numerable. Si Σ tiene algún modelo infinito, entonces Σ tiene modelos de cualquier cardinalidad infinita.

(b) Sea $\mathfrak{A}$ una estructura infinita para un lenguaje numerable. Entonces, para cualquier cardinal infinito λ, hay una estructura $\mathfrak{B}$ de cardinalidad λ tal que $\mathfrak{B} \equiv \mathfrak{A}$.

Demostración (a) Tome $\Gamma = \Sigma$, $\lambda = \aleph_0$ en el teorema.
(b) Tome $\Sigma = \text{Th}\,\mathfrak{A}$ en la parte (a). ⊣

Considere un conjunto Σ de enunciados, de los que se pensará que son axiomas no lógicos. (Por ejemplo, Σ podría ser un conjunto de axiomas de la teoría de conjuntos o un conjunto de axiomas de la teoría de los números.) Diremos que Σ es *categórica* sii cualesquiera dos modelos de Σ son isomorfos. El corolario anterior implica que si Σ tiene algún modelo infinito, entonces Σ no es categórica. Por ejemplo, no existe un conjunto de enunciados tal que sus modelos sean exactamente las estructuras isomorfas de $(\mathbb{N}; 0, S, +, \cdot)$. Esto constituye una limitación en la expresividad de los lenguajes de primer orden. (Como se verá en la sección 1 del capítulo IV, hay enunciados categóricos de segundo orden; sin embargo, los enunciados de segundo orden son objetos peculiares que se obtuvieron a costa de mantener fija la noción de *subconjunto*, inmune a la interpretación mediante estructuras.)

Teorías

Definimos una *teoría* como un conjunto de enunciados cerrado bajo implicación lógica. Esto es, T es una teoría sii T es un conjunto de enunciados tal que para cualquier enunciado σ del lenguaje,

$$T \models \sigma \Rightarrow \sigma \in T.$$

(Nótese que sólo admitimos enunciados, no fórmulas con variables libres.)

Por ejemplo, siempre habrá una teoría que sea la más pequeña, formada por los enunciados válidos del lenguaje. En el otro extremo está la teoría formada por todos lo enunciados del lenguaje, que es la única teoría que no es satisfactible.

Para una clase $\mathcal{K}$ de estructuras (para el lenguaje), definimos la *teoría* de $\mathcal{K}$ (que se escribe: Th $\mathcal{K}$) mediante la ecuación

$$\text{Th}\,\mathcal{K} = \{\sigma \mid \sigma \text{ es verdadero en cada elemento de } \mathcal{K}\}.$$

(Este concepto había surgido ya para el caso especial de $\mathcal{K} = \{\mathfrak{A}\}$.)

Teorema 26G Th $\mathcal{K}$ realmente es una teoría.

Demostración Cualquier elemento de $\mathcal{K}$ es un modelo de Th $\mathcal{K}$. De modo que si σ es verdadero en todo modelo de Th $\mathcal{K}$, entonces es verdadero en todo elemento de $\mathcal{K}$. De ahí que pertenezca a Th $\mathcal{K}$. ⊣

Por ejemplo, si los parámetros del lenguaje son $\forall$, **0**, **1**, $+$ y $\cdot$, y $\mathcal{F}$ es la clase de todos los campos, entonces Th $\mathcal{F}$, la teoría de los campos, simplemente es el conjunto de todos los enunciados del lenguaje que son verdaderos en todos los campos. Si $\mathcal{F}_0$ es la clase de campos de característica 0, entonces Th $\mathcal{F}_0$ es la teoría de campos de característica 0.

Recuérdese que para un conjunto de enunciados Σ, definimos Mod Σ como la clase de todos los modelos de Σ. Th Mod Σ es, entonces, el conjunto de todos los enunciados que son verdaderos en todos los modelos de Σ. Pero éste no es sino el conjunto de todos los enunciados implicados lógicamente por Σ. Llamemos a este conjunto el conjunto de *consecuencias* de Σ, Cn Σ. Entonces

$$\begin{aligned} \text{Cn}\,\Sigma &= \{\sigma \mid \Sigma \models \sigma\} \\ &= \text{Th Mod}\,\Sigma. \end{aligned}$$

Por ejemplo, la teoría de conjuntos es el conjunto de consecuencias de cierto conjunto de enunciados que, como es de esperarse, se conocen como los axiomas de la teoría de conjuntos. Un conjunto T de enunciados es una teoría sii $T = \text{Cn}\,T$.

Se dice que una teoría T es *completa* sii para cada enunciado σ, o bien $\sigma \in T$ o $(\neg\sigma) \in T$. Por ejemplo, para cualquier

estructura $\mathfrak{A}$, Th$\{\mathfrak{A}\}$ (que se escribe, igual que antes, como "Th $\mathfrak{A}$") siempre es una teoría completa. De hecho, reflexionando un poco, queda claro que Th $\mathcal{K}$ es una teoría completa sii cualesquiera dos elementos de $\mathcal{K}$ son elementalmente equivalentes. Y una teoría T es completa sii cualesquiera dos modelos de T son elementalmente equivalentes.

Por ejemplo, la teoría de campos no es completa, ya que los enunciados

$$1 + 1 = 0,$$
$$\exists x\, x \cdot x = 1 + 1$$

son verdaderos en algunos campos pero falsos en otros. La teoría de los campos algebraicamente cerrados de característica 0 es completa, pero esto de ninguna manera resulta obvio. (Véase el teorema 26J.)

*Definición Una teoría T es *axiomatizable* sii hay un conjunto decidible de enunciados Σ tal que $T = \text{Cn}\,\Sigma$.

Definición Una teoría T es *finitamente axiomatizable* sii $T = \text{Cn}\,\Sigma$ para algún conjunto finito de enunciados Σ.

En la segunda definición tenemos $T = \text{Cn}\{\sigma\}$ (que se escribe como "$T = \text{Cn}\,\sigma$") donde σ es la conjunción de la cantidad finita de elementos de Σ. Por ejemplo, la teoría de campos es finitamente axiomatizable, pues la clase de campos $\mathcal{F}$ es Mod Φ, donde Φ es el conjunto finito de los axiomas de campo. Y la teoría de campos es Th Mod $\Phi = \text{Cn}\,\Phi$.

La teoría de campos de característica 0 es axiomatizable, ya que es Cn Φ_0, donde Φ_0 consiste en los axiomas de campo (que son una cantidad finita) junto con los siguientes enunciados (que forman una cantidad infinita):

$$1 + 1 \neq 0,$$
$$1 + 1 + 1 \neq 0,$$
$$\cdots$$

Esta teoría no es finitamente axiomatizable. Para probar esto, primero hay que observar que ningún subconjunto finito de Φ_0 tiene a toda la teoría como el conjunto de sus consecuencias. (Ya que ese subconjunto finito sería verdadero en algún campo

de característica suficientemente grande.) Después aplique lo siguiente:

Teorema 26H Si $\mathrm{Cn}\,\Sigma$ es finitamente axiomatizable, entonces hay un $\Sigma_0 \subseteq \Sigma$ finito tal que $\mathrm{Cn}\,\Sigma_0 = \mathrm{Cn}\,\Sigma$.

Demostración Supongamos que $\mathrm{Cn}\,\Sigma$ es finitamente axiomatizable; entonces $\mathrm{Cn}\,\Sigma = \mathrm{Cn}\,\tau$ para algún enunciado τ. En general, $\tau \notin \Sigma$, pero al menos $\Sigma \models \tau$. ($\tau \in \mathrm{Cn}\tau = \mathrm{Cn}\,\Sigma$.) Por el teorema de compacidad hay un $\Sigma_0 \subseteq \Sigma$ finito tal que $\Sigma_0 \models \tau$. Entonces

$$\mathrm{Cn}\tau \subseteq \mathrm{Cn}\Sigma_0 \subseteq \mathrm{Cn}\Sigma,$$

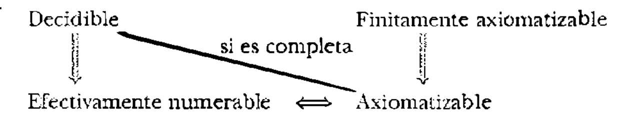
de modo que se cumple la igualdad. ⊣

Ahora podemos reformular los corolarios 25F y 25G de la siguiente manera:

***Corolario 26I** (a) Una teoría axiomatizable (en un lenguaje razonable) es efectivamente numerable.

(b) Una teoría completa axiomatizable (en un lenguaje razonable) es decidible.

Podemos representar las relaciones entre estos conceptos por medio de un diagrama (en el que hemos incluido los resultados del ejercicio 6):



Por ejemplo, una teoría a la que se ha dado una forma axiomática (tal como la teoría de conjuntos de Zermelo-Fraenkel, que no es sino $\mathrm{Cn}\,A_{ZF}$ para cierto conjunto A_{ZF}) es efectivamente numerable. En la sección 7 del capítulo III argumentaremos que la teoría de conjuntos (si es consistente) no es ni decidible ni completa. La teoría de los números, es decir, la teoría de la estructura $(\mathbb{N}; 0, S, <, +, \cdot, E)$, es completa pero no es efectivamente numerable, de donde no es axiomatizable (Secc. 5, Cap. III).

Podemos usar la parte (b) del corolario anterior para establecer la decidibilidad de una teoría axiomatizable, suponiendo que podamos mostrar que la teoría en cuestión es completa. En algunas ocasiones esto se puede hacer usando la prueba de completud de Łoś-Vaught.

Decimos que una teoría T es $\aleph_0$-*categórica* sii todos los modelos infinitos numerables de T son isomorfos. De manera más general, dado un cardinal κ, diremos que T es κ-categórica sii todos los modelos de T de cardinalidad κ son isomorfos.

Prueba de Łoś-Vaught (1954) Sea T una teoría en un lenguaje numerable. Supongamos que T no tiene modelos finitos.

(a) Si T es $\aleph_0$-categórica, entonces T es completa.

(b) Si T es κ-categórica para algún cardinal infinito κ, entonces T es completa.

Demostración Basta mostrar que $\mathfrak{A} \equiv \mathfrak{B}$ para cualesquiera dos modelos $\mathfrak{A}$ y $\mathfrak{B}$ de T. Como $\mathfrak{A}$ y $\mathfrak{B}$ son infinitos, existen (por el teorema LST) estructuras $\mathfrak{A}' \equiv \mathfrak{A}$ y $\mathfrak{B}' \equiv \mathfrak{B}$, con cardinalidad κ. $\mathfrak{A}'$ es isomorfa a $\mathfrak{B}'$, así que tenemos

$$\mathfrak{A} \equiv \mathfrak{A}' \cong \mathfrak{B}' \equiv \mathfrak{B}.$$

De modo que $\mathfrak{A} \equiv \mathfrak{B}$. ⊣

(Si T es una teoría en un lenguaje de cardinalidad λ, entonces debemos pedir que $\lambda \leq \kappa$.)

El inverso de la prueba de Łoś-Vaught es falso. Esto es, hay teorías completas que no son κ-categóricas para ningún κ.

En la sección 1 del capítulo III aplicaremos la prueba de Łoś-Vaught para probar la decidibilidad de la teoría de los números naturales con cero y sucesor. También se puede usar para probar la decidibilidad de la teoría del campo de los complejos. Pero esta prueba utilizará elementos de álgebra.

Teorema 26J (a) La teoría de campos algebraicamente cerrados de característica 0 es completa.

*(b) La teoría del campo de los complejos

$$\mathfrak{C} = (\mathbb{C}; 0, 1, +, \cdot)$$

es decidible.

Demostración Sea $\mathcal{A}$ la clase de los campos algebraicamente cerrados de característica 0. Entonces $\mathcal{A} = \text{Mod}(\Phi_0 \cup \Gamma)$, donde Φ_0 consiste, como antes, en los axiomas para campos de característica 0, y Γ consta de los enunciados

$$\forall a \, \forall b \, \forall c (a \neq 0 \to \exists x \; a \cdot x \cdot x + b \cdot x + c = 0),$$
$$\forall a \, \forall b \, \forall c \, \forall d (a \neq 0 \to \exists x \; a \cdot x \cdot x \cdot x + b \cdot x \cdot x + c \cdot x + d = 0),$$
$$\ldots$$

El conjunto $\Phi_0 \cup \Gamma$ es decidible y $\text{Th}\,\mathcal{A} = \text{Cn}(\Phi_0 \cup \Gamma)$, así que esta teoría es axiomatizable. La parte (a) del teorema afirma que la teoría también es completa y de ahí que sea decidible.

La parte (b) se sigue de la parte (a). Puesto que tenemos que $\mathfrak{C} \in \mathcal{A}$, de donde $\text{Th}\,\mathcal{A} \subseteq \text{Th}\,\mathfrak{C}$. La completud de $\text{Th}\,\mathcal{A}$ implica que la igualdad se cumple; véase el ejercicio 2.

Para demostrar la parte (a), aplicamos la prueba de Łoś-Vaught. Los modelos de $\text{Th}\,\mathcal{A}$ son exactamente los elementos de $\mathcal{A}$. Todos éstos son infinitos. Además afirmamos que $\text{Th}\,\mathcal{A}$ es categórica en cualquier cardinalidad no numerable. Esto equivale a decir que cualesquiera dos campos algebraicamente cerrados de característica 0 que tengan la misma cardinalidad no numerable son isomorfos.

Esta última afirmación es un resultado conocido dentro del álgebra. Presentaremos un bosquejo de la prueba para satisfacer el interés de aquellos lectores familiarizados con el tema. Cualquier campo $\mathfrak{F}$ se puede obtener de la siguiente manera: (1) Se empieza con el subcampo primo, el cual es determinado salvo isomorfismo por la característica de $\mathfrak{F}$. (2) Se toma una extensión trascendental, determinada salvo isomorfismo por la cardinalidad de la base de trascendencia, es decir, por el grado de trascendencia de $\mathfrak{F}$ (sobre su subcampo primo). (3) Finalmente, se toma alguna extensión algebraica. Y

así tenemos un teorema de Steinitz: dos campos algebraicamente cerrados son isomorfos sii tienen la misma característica y el mismo grado de trascendencia.

Si el grado de trascendencia de un campo infinito $\mathfrak{F}$ es κ, entonces la cardinalidad de $\mathfrak{F}$ es el mayor entre κ y $\aleph_0$. En consecuencia, para un campo no numerable, la cardinalidad es igual al grado de trascendencia. Así que podemos concluir, a partir del teorema de Steinitz, que si dos campos algebraicamente cerrados tienen la misma característica y la misma cardinalidad no numerable, entonces son isomorfos. ⊣

La teoría del campo de los reales

$$(\mathbb{R}; 0, 1, +, \cdot)$$

también es decidible. Pero este resultado (que se debe a Tarski) es mucho más profundo que el teorema anterior. La teoría del campo de los reales no es categórica en ninguna cardinalidad infinita, así que no se puede aplicar la prueba de Łoś-Vaught.

Como una última aplicación, podemos demostrar que el orden de los racionales es elementalmente equivalente al orden de los reales,

$$(\mathbb{Q}; <_Q) \equiv (\mathbb{R}; <_R),$$

donde $\mathbb{Q}$ y $\mathbb{R}$ son los racionales y los reales, respectivamente, y $<_Q$ y $<_R$ son los órdenes correspondientes. Para demostrar la equivalencia elemental, mostraremos que ambos son modelos de una teoría completa (de modo que esta última deberá coincidir con la teoría de cada estructura). El hecho clave lo provee un teorema de Cantor: cualesquiera dos órdenes lineales numerables, densos y sin extremos son isomorfos.

Para dar los detalles, debemos retroceder un poco. El lenguaje de este caso tiene igualdad y los parámetros $\forall$ y $<$. Sea δ la conjunción de los siguientes enunciados:

1. Axiomas de orden (tricotomía y transitividad):

$$\forall x \forall y\, (x < y \vee x = y \vee y < x),$$
$$\forall x \forall y\, (x < y \rightarrow y \not< x),$$
$$\forall x \forall y \forall z\, (x < y \rightarrow y < z \rightarrow x < z).$$

2. Densidad:

$$\forall x \forall y\,(x < y \to \exists z\,(x < z < y)).$$

3. Sin extremos

$$\forall x\, \exists y\, \exists z\, (y < x < z).$$

Los órdenes lineales densos y sin extremos son, por definición, las estructuras para este lenguaje que son modelos de δ. Está claro que todos son infinitos. Además, afirmamos que la teoría de estos órdenes, $\mathrm{Cn}\,\delta$, es $\aleph_0$-categórica. Esto surge del siguiente resultado:

Teorema 26K (Cantor) Cualquier modelo numerable de δ es isomorfo a $(\mathbb{Q}; <_Q)$.

Dejamos la demostración para el ejercicio 4.

Ahora podemos aplicar la prueba de Łoś-Vaught para concluir que $\mathrm{Cn}\,\delta$ es completa. Y de aquí que cualesquiera dos modelos de δ sean elementalmente equivalentes; en particular,

$$(\mathbb{Q}; <_Q) \equiv (\mathbb{R}; <_R).$$

También podemos concluir que estas dos estructuras tienen teorías decidibles.

Forma normal prenex

A veces resulta conveniente mover todos los símbolos de cuantificación a la izquierda de los otros símbolos. Por ejemplo,

$$\forall x\,(Ax \to \forall y\, Bxy)$$

es equivalente a

$$\forall x \forall y\,(Ax \to Bxy).$$

Y

$$\forall x\,(Ax \to \exists y\, Bxy)$$

es equivalente a

$$\forall x\, \exists y\,(Ax \to Bxy).$$

Definimos una fórmula *prenex* como aquella con la forma

$$Q_1 x_1 \cdots Q_n x_n\, \alpha,$$

(para algún $n \geq 0$), donde Q_i es $\forall$ o $\exists$ y α no tiene cuantificadores.

Teorema de la forma normal prenex Para cualquier fórmula podemos encontrar una fórmula prenex lógicamente equivalente.

Demostración Haremos uso de las siguientes reglas de manipulación de cuantificadores.

Q1a. $\neg \forall x\, \alpha \models\!\!\!\Rightarrow\!\!\models \exists x \neg \alpha$.

Q1b. $\neg \exists x\, \alpha \models\!\!\!\Rightarrow\!\!\models \forall x \neg \alpha$.

Q2a. $(\alpha \to \forall x\, \beta) \models\!\!\!\Rightarrow\!\!\models \forall x\, (\alpha \to \beta)$ para x no libre en α.

Q2b. $(\alpha \to \exists x\, \beta) \models\!\!\!\Rightarrow\!\!\models \exists x\, (\alpha \to \beta)$ para x no libre en α.

Q3a. $(\forall x\, \alpha \to \beta) \models\!\!\!\Rightarrow\!\!\models \exists x\, (\alpha \to \beta)$ para x no libre en β.

Q3b. $(\exists x\, \alpha \to \beta) \models\!\!\!\Rightarrow\!\!\models \forall x\, (\alpha \to \beta)$ para x no libre en β.

Q1 es clara; para las otras, véanse los ejemplos de la sección 4 de este capítulo y el ejercicio 8 de esa sección.

Ahora, mediante inducción, demostraremos que toda fórmula tiene una fórmula prenex equivalente.

1. Para fórmulas atómicas no hay nada que hacer, ya que cualquier fórmula sin cuantificadores es trivialmente una fórmula prenex.

2. Si α es equivalente a la fórmula prenex α', entonces $\forall x\, \alpha$ es equivalente a la fórmula prenex $\forall x\, \alpha'$.

3. Si α es equivalente a la fórmula prenex α', entonces $\neg \alpha$ es equivalente a $\neg \alpha'$. Aplique Q1 a $\neg \alpha'$ para obtener una fórmula prenex; por ejemplo,

$$\neg \forall x \exists y \exists z\, \beta \models\!\!\!\Rightarrow\!\!\models \exists x \forall y \forall z \neg \beta.$$

4. Finalmente llegamos al caso de $\alpha \to \beta$. Por hipótesis inductiva tenemos fórmulas prenex α' y β' que son equivalentes a α y a β, respectivamente. Gracias a los teoremas con que contamos sobre variantes alfabéticas, podemos incluso suponer que cualquier variable que ocurre cuantificada en una de las fórmulas α' o β' no ocurre en la otra. Después usamos Q2 y Q3 para obtener una fórmula prenex equivalente a $\alpha' \to \beta'$ (y por

lo tanto a $\alpha \to \beta$). Nótese que hay cierto grado de libertad en el orden en que se aplican las reglas Q2 y Q3. Por ejemplo, la fórmula

$$\forall x \, \exists y \, \varphi \to \exists u \, \psi$$

(donde x y y no ocurren en ψ, u no ocurre en φ) es equivalente a cualquiera de las siguientes fórmulas:

$$\exists x \, \forall y \, \exists u \, (\varphi \to \psi),$$
$$\exists x \, \exists u \, \forall y \, (\varphi \to \psi),$$
$$\exists u \, \exists x \, \forall y \, (\varphi \to \psi). \qquad \dashv$$

Retrospectiva

Al comienzo de este libro se dijo que la lógica simbólica es un modelo matemático del pensamiento deductivo. Éste es un buen momento para reflexionar acerca de dicha afirmación, a la luz del material tratado hasta ahora.

Como primer ejemplo, consideremos a un matemático trabajando en la teoría de conjuntos. Él usa un lenguaje con un símbolo de igualdad, un símbolo $\in$ para la pertenencia y un buen número de símbolos definidos ($\emptyset$, $\cup$ y otros). En principio, los símbolos definidos podrían ser eliminados y cualquier enunciado podría ser reemplazado por un enunciado equivalente en el que no aparezcan los símbolos definidos. (En relación con esto, véase la sección 7 de este capítulo, donde se trata este tema sistemáticamente.) Este matemático toma como nociones primitivas (o indefinidas) los conceptos de conjunto y de pertenencia. Adopta algún conjunto de axiomas A_{TC} en el que intervienen estos conceptos. De ciertos enunciados (sus teoremas), afirma que son verdaderos siempre y cuando los axiomas sean verdaderos, independientemente de lo que signifiquen las nociones indefinidas de conjunto y pertenencia. Para apoyar sus afirmaciones, ofrece demostraciones, las cuales son argumentos de extensión finita que pretenden convencer a sus colegas de la correctud de sus afirmaciones.

En términos de lógica de primer orden podemos describir todo esto como sigue: el lenguaje es de primer orden con igualdad y con un símbolo de predicado $\in$ de dos argumentos.

Entonces, $\forall$ y $\in$ son los únicos parámetros abiertos a la interpretación. En este lenguaje, hay un conjunto A_{TC} de enunciados seleccionados para ser el conjunto de axiomas (no lógicos). Después, otros enunciados son consecuencias lógicas de A_{TC}, es decir, son verdaderos en cualquier modelo de A_{TC}. Si τ es una consecuencia de A_{TC} (y sólo entonces), hay una deducción de τ a partir de A_{TC}.

Piense ahora en un caso más típico del hipotético matemático activo: el del algebrista o el del analista. El algebrista usa axiomas para (digamos) la teoría de grupos, pero también utiliza una parte de la teoría de conjuntos. De manera similar, el analista trabaja con enunciados que involucran tanto números como conjuntos de números. En ambos casos es ampliamente reconocido que uno puede, en principio, convertir las afirmaciones del álgebra y del análisis en afirmaciones de la teoría de conjuntos. De modo que las observaciones que se hicieron en el párrafo anterior también se aplican a estos casos.

El interés que la lógica simbólica tiene para el matemático se debe en gran parte a la precisión con la que ésta refleja las deducciones matemáticas. A la larga, seguramente será útil para entender los procesos fundamentales que encierra el quehacer matemático.

Aún queda pendiente la cuestión acerca de la precisión con la que la lógica de primer orden refleja el pensamiento deductivo no matemático. La lógica, simbólica y no simbólica, ha sido una constante en el estudio filosófico del proceso mediante el cual la gente llega a sostener ciertas ideas. Una vasta gama de situaciones superficiales provee ejemplos no matemáticos en los que se aplica la lógica de primer orden. Lewis Carroll dio algunos de ellos, uno de los cuales infería, a partir de tres hipótesis, que los bebés no podían manipular cocodrilos: (1) los bebés son ilógicos; (2) nadie que pueda manipular un cocodrilo puede ser menospreciado; (3) las personas ilógicas son menospreciadas.

Pero, ¿qué pasa con las situaciones no tan superficiales? Aquí la aplicabilidad se oscurece por el hecho de que no solemos hacer explícitas las suposiciones que usamos para sacar conclusiones. Hay áreas específicas (en diversos campos como la física, la medicina y el derecho) en las que las suposicio-

nes no sólo se pueden hacer explícitas, sino que de hecho se mencionan. En algunos casos parece que no se necesita toda la fuerza de la lógica de primer orden para formalizar las deducciones de la vida real; sin embargo, posiblemente en otros casos, que abarcan desde la vida cotidiana hasta la mecánica cuántica, podrían ser necesarias más características.

Ejercicios

1. Demuestre que los siguientes enunciados son finitamente válidos (es decir, que son verdaderos en toda estructura finita):

   (a) $\exists x \exists y \exists z\, [(P x f x \to P x x) \lor (P x y \land P y z \land \neg P x z)]$

   (b) $\exists x \forall y \exists z\, [(Q z x \to Q z y) \to (Q x y \to Q x x)]$

   Sugerencia: Demuestre que cualquier modelo de la negación debe ser infinito.

2. Sean T_1 y T_2 teorías (en el mismo lenguaje) tales que (i) $T_1 \subseteq T_2$, (ii) T_1 es completa, y (iii) T_2 es satisfactible. Demuestre que $T_1 = T_2$.

3. Demuestre los siguientes resultados:

   (a) $\Sigma_1 \subseteq \Sigma_2 \Rightarrow \text{Mod}\,\Sigma_2 \subseteq \text{Mod}\,\Sigma_1$.

   $\mathcal{K}_1 \subseteq \mathcal{K}_2 \Rightarrow \text{Th}\,\mathcal{K}_2 \subseteq \text{Th}\,\mathcal{K}_1$.

   (b) $\Sigma \subseteq \text{Th Mod}\,\Sigma$ y $\mathcal{K} \subseteq \text{Mod Th}\,\mathcal{K}$.

   (c) $\text{Mod}\,\Sigma = \text{Mod Th Mod}\,\Sigma$ y $\text{Th}\,\mathcal{K} = \text{Th Mod Th}\,\mathcal{K}$. (La parte (c) se sigue de (a) y (b).)

4. Pruebe que cualesquiera dos órdenes lineales numerables, densos y sin extremos son isomorfos (Teorema 26K). *Sugerencias:* Sean $\mathfrak{A}$ y $\mathfrak{B}$ tales estructuras con $|\mathfrak{A}| = \{a_0, a_1, \ldots\}$ y $|\mathfrak{B}| = \{b_0, b_1, \ldots\}$. Construya un isomorfismo paso a paso; en el paso $2n$ asegúrese de que a_n va emparejada con algún b_j adecuado, y en el paso $2n + 1$ asegúrese de que b_n va emparejado con alguna a_i adecuada.

5. Encuentre fórmulas prenex equivalentes a los siguientes enunciados.

(a) $(\exists x\, A\, x \wedge \exists x\, B x) \rightarrow C\, x$.

(b) $\forall x\, A\, x \leftrightarrow \exists x\, B\, x$.

*6. Pruebe el inverso del inciso (a) del Corolario 26I: una teoría efectivamente numerable (en un lenguaje razonable) es axiomatizable. *Sugerencia:* El conjunto $\{\sigma_0, \sigma_1, \sigma_2, \ldots\}$ es equivalente (en el sentido de que tiene los mismos modelos) al conjunto $\{\sigma_0, \sigma_0 \wedge \sigma_1, \sigma_0 \wedge \sigma_1 \wedge \sigma_2, \ldots\}$.

7. Considere un lenguaje con un símbolo de predicado $<$ de dos argumentos y sea $\mathfrak{N} = (\mathbb{N}; <)$ la estructura que consiste en los números naturales con su orden usual. Muestre que hay alguna $\mathfrak{A}$ elementalmente equivalente a $\mathfrak{N}$ tal que $<^{\mathfrak{A}}$ tiene una cadena descendente. (Esto es, debe haber $a_0, a_1, \ldots$ en $|\mathfrak{A}|$ tal que $\langle a_{i+1}, a_i \rangle \in <^{\mathfrak{A}}$ para toda i.) *Sugerencia:* Aplique el teorema de compacidad.

Comentario: El objetivo de este ejercicio es demostrar que en este lenguaje *no* se puede expresar "No hay cadena descendente".

8. Suponga que σ es verdadero en todos los modelos infinitos de una teoría T. Demuestre que hay un número finito k tal que σ es verdadero en todos los modelos $\mathfrak{A}$ de T para los cuales $|\mathfrak{A}|$ tiene k o más elementos.

9. Decimos que un conjunto Σ de enunciados tiene la ***propiedad del modelo finito*** sii todo elemento σ de Σ que tenga algún modelo tiene un modelo finito. Supongamos que Σ es un conjunto de enunciados en un lenguaje finito (es decir, un lenguaje con una cantidad finita de parámetros) y que Σ tiene la propiedad del modelo finito. Formule un procedimiento efectivo tal que, dado cualquier elemento σ de Σ, decida si σ tiene algún modelo. *Sugerencia:* ¿Es el conjunto de dichos enunciados efectivamente numerable? ¿Es su complemento efectivamente numerable?

10. Supongamos que tenemos un lenguaje finito sin símbolos de función.

(a) Demuestre que el conjunto de enunciados $\exists_2$ satisfactibles es decidible. (Véase el ejercicio 19 de la sec-

ción 2 de este capítulo para la terminología y los antecedentes.) *Sugerencia:* Aplique el ejercicio anterior.

(b) Demuestre que el conjunto de enunciados $\forall_2$ válidos es decidible. (Una fórmula $\forall_2$ es de la forma $\forall x_1 \cdots \forall x_m \exists y_1 \cdots \exists y_n\, \theta$, donde θ es una fórmula sin cuantificadores.)

Observaciones: En la lógica de primer orden, el "problema de la decisión" (*Entscheidungsproblem*) es el problema de decidir, dada una fórmula, si es válida o no. Por el teorema de Church (Secc. 5, Cap. III), en general, este problema no tiene solución. Este ejercicio da un subcaso del problema de la decisión que sí puede ser resuelto.

7. *Interpretaciones entre teorías*[5]

En algunos casos se puede demostrar que una teoría T_1 es en todos sentidos tan poderosa como otra teoría T_0. Evidentemente esto sucede si las teorías están en el mismo lenguaje y $T_0 \subseteq T_1$. Pero incluso si las teorías están en lenguajes diferentes, puede existir una traducción de un lenguaje a otro de modo tal que los elementos de T_0 se traduzcan como elementos de T_1. Este tipo de situación es lo que examinaremos en esta sección.

Comenzaremos abordando el tema de los símbolos definidos. Este tema, además de ser en sí mismo muy interesante, servirá de ejemplo para la situación del párrafo anterior, donde T_0 se construye a partir de T_1 agregando un nuevo símbolo definido. Si la definición se hace adecuadamente, la teoría original T_1 deberá, en principio, ser tan fuerte como la nueva T_0. Consideraremos únicamente el caso de los símbolos de función definidos, ya que el caso de los símbolos de predicado definidos no presenta, en comparación, verdaderas dificultades.

Definición de funciones

Con frecuencia es útil en matemáticas introducir definiciones de funciones nuevas. Por ejemplo, en la teoría de conjuntos

[5] Los resultados de esta sección se utilizarán únicamente en la última parte de la sección 7 del capítulo III.

se define la operación de conjunto potencia $\mathcal{P}$ mediante un enunciado como "Sea $\mathcal{P}x$ el conjunto cuyos elementos son los subconjuntos de x". O bien, por medio de un enunciado en lenguaje formal (que contiene $\in$, $\subseteq$ y $\mathcal{P}$),

$$\forall v_1 \forall v_2 \, [\mathcal{P} v_1 = v_2 \leftrightarrow \forall u (u \in v_2 \leftrightarrow u \subseteq v_1)].$$

Ahora bien, las definiciones no son iguales a los teoremas ni a los axiomas. A diferencia de los teoremas, las definiciones no son cosas que probemos; simplemente las declaramos de manera arbitraria. Sin embargo, a diferencia de los axiomas, no esperamos que las definiciones agreguen información sustantiva. Se espera que una definición nos facilite las cosas, no que agregue nada nuevo a nuestro conocimiento.

Ahora bien, para que una definición realmente nos facilite las cosas deberá ser razonable. A continuación daremos un ejemplo de lo que sería una definición nada razonable dentro de la teoría de los números. Suponga que introducimos un nuevo símbolo de función mediante la "definición"

$$f(x) = y \quad \text{sii} \quad x < y.$$

(O mediante el enunciado en lenguaje formal: $\forall v_1, \forall v_2 (f v_1 = v_2 \leftrightarrow v_1 < v_2)$.) Como sabemos que $1 < 2$, tenemos que $f(1) = 2$. Pero también $1 < 3$, así que $f(1) = 3$. Y así llegamos a la conclusión (que en sí misma no involucra a f) de que $2 = 3$.

Obviamente, esta definición de f es en cierto sentido muy mala. No sólo nos facilitó las cosas; también nos permitió concluir que $2 = 3$, lo cual no se podría hacer sin esa definición. El problema es que la definición da el nombre "$f(1)$" de manera ambigua a varias cosas (entre ellas al 2 y al 3); por lo que $f(1)$ no está "bien definida". Los nombres deben designar objetos únicos.

En esta subsección queremos examinar las condiciones bajo las cuales podamos estar seguros de que una definición es buena. Para simplificar la notación, consideraremos únicamente la definición de un símbolo de función f de un argumento, pero las observaciones se aplicarán también a los símbolos de función de n argumentos.

Considere una teoría T en un lenguaje que no tenga todavía el símbolo de función f de un argumento. (Por ejemplo, T podría ser el conjunto de las consecuencias de los axiomas que el lector prefiera de la teoría de conjuntos.) Queremos agregar f al lenguaje, introduciéndolo mediante la definición

$$\forall v_1 \forall v_2 \, [f v_1 = v_2 \leftrightarrow \varphi], \tag{δ}$$

donde φ es una fórmula en el lenguaje original (es decir, una fórmula que no contiene a f) en la que sólo v_1 y v_2 pueden ser variables libres.

Teorema 27A En la situación anterior, las siguientes afirmaciones son equivalentes:

(a) (La definición no es creativa.) Para cualquier enunciado σ en el lenguaje original, si

$$T; \delta \models \sigma$$

(en el lenguaje aumentado), entonces $T \models \sigma$.

(b) (f está bien definida.) El enunciado

$$\forall v_1 \exists ! v_2 \, \varphi \tag{ε}$$

está en la teoría T. (En este caso, "$\exists ! v_2 \, \varphi$" es una abreviación de una fórmula más larga; véase el ejercicio 21 de la sección 2 de este capítulo.)

Demostración Para ver que (a) $\Rightarrow$ (b), simplemente hay que observar que $\delta \models \varepsilon$. Así que si tomamos $\sigma = \varepsilon$ en la parte (a), obtenemos $T \models \varepsilon$.

Para el inverso, supongamos que $T \models \varepsilon$. Sea $\mathfrak{A}$ un modelo de T. ($\mathfrak{A}$ es una estructura para el lenguaje original.) Para $d \in |\mathfrak{A}|$, sea $F(d)$ la única $e \in |\mathfrak{A}|$ tal que $\models_{\mathfrak{A}} \varphi[[d, e]]$. (Dicha e es única, pues $\models_{\mathfrak{A}} \varepsilon$.) Sea $(\mathfrak{A}, F)$ la estructura del lenguaje aumentado que coincide con $\mathfrak{A}$ en los parámetros originales y que asigna F al símbolo f. Entonces es fácil ver que $(\mathfrak{A}, F)$ es un modelo de δ. Más aún, $\mathfrak{A}$ y $(\mathfrak{A}, F)$ satisfacen los mismos enunciados del lenguaje original. En particular, $(\mathfrak{A}, F)$ es un modelo de T. De modo que

$$
\begin{aligned}
T; \delta \models \sigma &\Rightarrow \models_{(\mathfrak{A}, F)} \sigma \\
&\Rightarrow \models_{\mathfrak{A}} \sigma. \qquad \dashv
\end{aligned}
$$

(Este argumento se puede simplificar usando la lógica de segundo orden. ε es lógicamente equivalente al enunciado $\exists f \delta$.)

Interpretaciones

La idea básica es que una teoría puede ser tan fuerte (en un sentido que se precisará más adelante) como cualquier otra teoría en otro lenguaje. Cuando se manejan dos lenguajes simultáneamente, es importante evitar conflictos entre ellos; por ejemplo, el símbolo de negación en un lenguaje no deberá ser un símbolo de predicado en el otro. Podemos eliminar dichos conflictos si suponemos que cada uno de los lenguajes se obtiene, a partir de un tercer lenguaje original, eliminando algunos parámetros (y tal vez la igualdad).

Por ejemplo, la teoría axiomática de conjuntos es al menos tan fuerte como la teoría de los números naturales con cero y sucesor, es decir, la teoría de $(\mathbb{N}; 0, S)$. Cualquier enunciado en el lenguaje de $(\mathbb{N}; 0, S)$ puede ser traducido de manera natural a un enunciado de la teoría de conjuntos. (Esta traducción se bosqueja brevemente en la sección 7 del capítulo III.) Si el enunciado original es verdadero en $(\mathbb{N}; 0, S)$, entonces la traducción será una consecuencia de los axiomas de la teoría de conjuntos. (Esto no es obvio. La prueba usa resultados que se desarrollarán en la sección 1 del capítulo III.)

Veamos el segundo ejemplo con mayor detalle. Por un lado, considere la teoría de

$$(\mathbb{N}; 0, S)$$

en su lenguaje, y por el otro, la teoría de

$$(\mathbb{Z}; +, \cdot)$$

en su lenguaje. (Aquí $\mathbb{Z}$ es el conjunto de todos los enteros, positivos, negativos y cero.) Dentro de poco podremos afirmar que la segunda teoría es tan fuerte como la primera. ¿Cómo se puede traducir un enunciado sobre los números naturales $\mathbb{N}$ con 0 y S a un enunciado sobre los enteros $\mathbb{Z}$ con suma y multiplicación?

La primera pista nos la da el teorema de Lagrange para la teoría de los números: un entero es no negativo sii es la suma de cuatro cuadrados. De modo que un cuantificador $\forall x$ en el primer lenguaje (en donde se pretende que x corra sobre $\mathbb{N}$) se puede sustituir por

$$\forall x\ (\exists y_1\ \exists y_2\ \exists y_3\ \exists y_4\ x = y_1 \cdot y_1 + y_2 \cdot y_2 + y_3 \cdot y_3 + y_4 \cdot y_4 \rightarrow$$

en el segundo lenguaje.

La segunda pista es que $\{0\}$ y la función sucesor (vista como una relación) son definibles en $(\mathbb{Z}; +, \cdot)$. El conjunto $\{0\}$ está definido por

$$v_1 + v_1 = v_1.$$

La relación de sucesor (extendida a $\mathbb{Z}$) está definida por

$$\forall z\ (z \cdot z = z \wedge z + z \neq z \rightarrow v_1 + z = v_2).$$

Por lo tanto, el enunciado sobre $(\mathbb{N}; 0, S)$

$$\forall x S x \neq 0$$

puede traducirse como

$$\forall x [\exists y_1\ \exists y_2\ \exists y_3\ \exists y_4\ x = y_1 \cdot y_1 + y_2 \cdot y_2 + y_3 \cdot y_3 + y_4 \cdot y_4 \rightarrow$$
$$\neg \forall u\ (u + u = u \rightarrow \forall v\ (\forall z\ (z \cdot z = z \wedge z + z \neq z \rightarrow x + z = v)$$
$$\rightarrow v = u))].$$

Hasta aquí llegamos con los ejemplos. Para nuestra discusión general, nos servirá introducir la siguiente notación

$$\varphi(t) = \varphi_t^{v_1},$$
$$\varphi(t_1, t_2) = (\varphi_{t_1}^{v_1})_{t_2}^{v_2},$$

y así sucesivamente. Por lo tanto, $\varphi = \varphi(v_1) = \varphi(v_1, v_2)$. Si usamos "$\varphi(x)$", no nos preocupará mucho si x es o no sustituible por v_1 en φ. Si no lo es, entonces haremos que $\varphi(x)$ sea $\psi_x^{v_1}$, donde ψ es una variante alfabética adecuada de φ.

Supongamos ahora que estamos ante la siguiente situación general:

L_0 es un lenguaje. (Para todos los propósitos prácticos, un *lenguaje* puede ser un conjunto de parámetros, posiblemente aumentado con el símbolo de igualdad.)

T_1 es una teoría en un lenguaje (posiblemente diferente) L_1, que incluye la igualdad.

Definición Una *interpretación* π de L_0 en T_1 es una función definida sobre el conjunto de parámetros de L_0, tal que

1. π asigna a $\forall$ una fórmula $\pi_\forall$ de L_1 en la que a lo más v_1 ocurre libre, y es tal que

$$\text{(i)} \qquad T_1 \models \exists v_1\, \pi_\forall.$$

(La idea es que en cualquier modelo de T_1, la fórmula $\pi_\forall$ defina un conjunto no vacío que será usado como el universo de una estructura para L_0.)

2. π asigna a cada parámetro predicado P de n argumentos una fórmula π_P de L_1 en la que a lo más las variables $v_1, \ldots, v_n$ ocurren libres.

3. π asigna a cada símbolo de función f de n argumentos una fórmula π_f de L_1, en la que a lo más $v_1, \ldots, v_n, v_{n+1}$ ocurren libres, y tal que

$$\text{(ii)} \quad \begin{array}{l} T_1 \models \forall v_1 \cdots \forall v_n\, (\pi_\forall(v_1) \to \cdots \to \pi_\forall(v_n) \to \\ \quad \exists x\, (\pi_\forall(x) \wedge \forall v_{n+1}(\pi_f(v_1, \ldots, v_{n+1}) \leftrightarrow v_{n+1} = x))). \end{array}$$

(En español, esta fórmula significa: "Para toda $\vec{v}$ en el conjunto definido por $\pi_\forall$, hay una única x tal que $\pi_f\,(\vec{v}, x)$, y además x está en el conjunto definido por $\pi_\forall$." La idea es asegurar que en cualquier modelo de T_1, π_f define una función sobre el universo definido por $\pi_\forall$. En el caso de un símbolo de constante c, tenemos $n = 0$ y (ii) se convierte en

$$T_1 \models \exists x\, (\pi_\forall(x) \wedge \forall v_1\, (\pi_c(v_1) \leftrightarrow v_1 = x)).$$

En otras palabras, π_c define un conjunto unitario cuyo único elemento también está en el conjunto definido por $\pi_\forall$.)

Por ejemplo, si L_0 es el lenguaje de $(\mathbb{N}; 0, S)$ y T_1 es la teoría de $(\mathbb{Z}; +, \cdot)$, entonces tenemos

$$\pi_\forall(x) = \exists y_1\, \exists y_2\, \exists y_3\, \exists y_4\; x = y_1 \cdot y_1 + y_2 \cdot y_2 + y_3 \cdot y_3 + y_4 \cdot y_4,$$

$$\pi_0(x) = x + x = x,$$
$$\pi_S(x, y) = \forall z\,(z \cdot z = z \wedge z + z \neq z \rightarrow x + z = y).$$

(Aquí estamos explotando el hecho de que en $(\mathbb{Z}; +, \cdot)$ podemos, en efecto, definir la estructura $(\mathbb{N}; 0, S)$.)

Si L_0 coincide con L_1, trivialmente se tiene a π como la interpretación identidad, para la cual

$$\pi_\forall = v_1 = v_1,$$
$$\pi_P = P\,v_1 \cdots v_n,$$
$$\pi_f = f\,v_1 \cdots v_n = v_{n+1}.$$

Las condiciones (i) y (ii) entonces se cumplen sin importar qué sea T_1.

Ahora supongamos que π es una interpretación y sea $\mathfrak{B}$ un modelo de T_1. Hay una manera natural de extraer de $\mathfrak{B}$ una estructura ${}^\pi\mathfrak{B}$ para L_0. A saber, sea

$$|{}^\pi\mathfrak{B}| = \text{el conjunto definido en } \mathfrak{B} \text{ por } \pi_\forall,$$
$$P^{{}^\pi\mathfrak{B}} = \text{la relación definida en } \mathfrak{B} \text{ por } \pi_P, \text{ restringida a } |{}^\pi\mathfrak{B}|,$$
$$f^{{}^\pi\mathfrak{B}}(a_1, \ldots, a_n) = \text{la única } b \text{ tal que } \models_\mathfrak{B} \pi_f[\![a_1, \ldots, a_n, b]\!], \text{ donde } a_1, \ldots, a_n \text{ están en } |{}^\pi\mathfrak{B}|.$$

Por la condición (i) de la definición de interpretación, $|{}^\pi\mathfrak{B}| \neq \emptyset$. Y por la condición (ii), la definición de $f^{{}^\pi\mathfrak{B}}$ tiene sentido; es decir, hay una única b que cumple la condición anterior. Por lo tanto, ${}^\pi\mathfrak{B}$ es, de hecho, una estructura para el lenguaje L_0.

Definamos el conjunto $\pi^{-1}[T_1]$ de enunciados de L_0 mediante la ecuación

$$\pi^{-1}[T_1] = \mathrm{Th}\,\{{}^\pi\mathfrak{B} \mid \mathfrak{B} \in \mathrm{Mod}\,T_1\}$$
$$= \{\sigma \mid \sigma \text{ es un enunciado de } L_0 \text{ verdadero en toda estructura } {}^\pi\mathfrak{B} \text{ obtenida a partir de un modelo } \mathfrak{B} \text{ de } T_1\}.$$

Ésta *es* una teoría, como lo es $\mathrm{Th}\,\mathcal{K}$ para cualquier clase $\mathcal{K}$. Es una teoría satisfactible sii T_1 es satisfactible.

Ejemplo Al principio de esta sección teníamos una teoría T que contenía el enunciado

$$\forall v_1\, \exists! v_2\, \varphi \qquad (\varepsilon)$$

Aumentamos el lenguaje a un lenguaje más grande L^+ que contenía un símbolo de función f. La "definición" de f se obtenía del enunciado de L^+

$$\forall v_1 \forall v_2 [f v_1 = v_2 \leftrightarrow \varphi] \qquad (\delta)$$

Hemos mostrado que para un enunciado σ en el lenguaje original de T, si $T; \delta \models \sigma$, entonces $T \models \sigma$.

Tenemos una interpretación π de L^+ en T. π es la interpretación identidad en todos los parámetros excepto f. La fórmula π_f es φ. El hecho de que $T \models \varepsilon$ es justo lo que necesitamos para verificar que π es de verdad una interpretación. Para cualquier modelo $\mathfrak{A}$ de T, ${}^{\pi}\mathfrak{A}$ es una estructura que antes llamamos $(\mathfrak{A}, F)$, y es un modelo de $T; \delta$.

Afirmamos que

$$\pi^{-1}[T] = \text{Cn}\,(T; \delta).$$

Primero observemos que cualquier modelo $\mathfrak{B}$ de $T; \delta$ es igual a ${}^{\pi}\mathfrak{A}$, donde $\mathfrak{A}$ es la restricción de $\mathfrak{B}$ al lenguaje de T. Así que para un enunciado σ de L^+,

$$\begin{aligned} \sigma \in \pi^{-1}[T] &\Leftrightarrow \models_{\pi\mathfrak{A}} \sigma && \text{para todo modelo } \mathfrak{A} \text{ de } T \\ &\Leftrightarrow \models_{\mathfrak{B}} \sigma && \text{para todo modelo } \mathfrak{B} \text{ de } T; \delta \\ &\Leftrightarrow T; \delta \models \sigma. \end{aligned}$$

Traducción sintáctica

En la subsección anterior sobre interpretaciones hablamos de modelos arbitrarios y otros conceptos semánticos. Pero el lector tal vez ya se haya percatado de que hay algo muy concreto que se puede decir con respecto a una interpretación π de L_0 en T_1. Brevemente: dada una fórmula φ de L_0, podemos encontrar una fórmula φ^{π} de L_1 que de alguna manera corresponda exactamente a φ. Definimos φ^{π} por recursión sobre φ.

Primero consideremos una fórmula atómica α de L_0. Por ejemplo, si α es

$$P f g x,$$

entonces α es lógicamente equivalente a

$$\forall y\,(gx = y \rightarrow \forall z\,(f y = z \rightarrow Pz)).$$

Y podemos tomar α^π como la fórmula de L_1

$$\forall y\ (\pi_g(x,y) \to \forall z\ (\pi_f(y,z) \to \pi_P(z))).$$

En general, examinemos de derecha a izquierda una fórmula atómica α. En el lugar más a la derecha en el que aparezca un símbolo de función se inicia un segmento de la forma $gx_1 \cdots x_n$, para alguna g de n argumentos. (En el ejemplo, $n = 1$.) Reemplace este segmento con alguna nueva variable y, y agregue como prefijo $\forall y\ (\pi_g(x_1, \ldots, x_n, y) \to$. Continúe con el siguiente lugar en el que ocurra un símbolo de función. Finalmente, reemplace el símbolo de predicado P (si es un parámetro) por π_P (con las variables adecuadas).

La definición de α^π puede formularse con mayor precisión usando recursión sobre el número de lugares en los que aparecen símbolos de función en α. Si ese número es cero, entonces α es $P\ x_1 \cdots x_n$ y α^π es $\pi_P(x_1, \ldots, x_n)$. De otra manera, tome el lugar más a la derecha en el que aparezca un símbolo de función g. Si g es un símbolo de n argumentos, entonces en ese lugar se inicia un segmento $g\,x_1 \cdots x_n$. Reemplace este segmento con alguna nueva variable y, para obtener una fórmula que podemos llamar $\alpha_y^{gx_1\cdots x_n}$. Entonces α^π es

$$\forall y\ (\pi_g(x_1, \ldots, x_n, y) \to (\alpha_y^{gx_1\cdots x_n})^\pi).$$

Por ejemplo,

$$\begin{aligned}(P\,f\,gx)^\pi &= \forall y\ (\pi_g(x,y) \to (Pfy)^\pi) \\ &= \forall y\ (\pi_g(x,y) \to \forall z\ (\pi_f(y,z) \to (Pz)^\pi)) \\ &= \forall y\ (\pi_g(x,y) \to \forall z\ (\pi_f(y,z) \to \pi_P(z))).\end{aligned}$$

La interpretación de una fórmula no atómica se define como es de esperarse. $(\neg\varphi)^\pi$ es $(\neg\varphi^\pi)$, $(\varphi \to \psi)^\pi$ es $(\varphi^\pi \to \psi^\pi)$, y $(\forall x\varphi)^\pi$ es $\forall x\ (\pi_\forall(x) \to \varphi^\pi)$. (De modo que los cuantificadores están "relativizados" a $\pi_\forall$.)

El sentido en el que φ^π "dice lo mismo" que φ se precisa en el siguiente lema básico.

Lema 27B Sea π una interpretación de L_0 en T_1, y sea $\mathfrak{B}$ un modelo de T_1. Para cualquier fórmula φ de L_0 y cualquier función s de las variables en $|^\pi\mathfrak{B}|$,

$$\models_{^\pi\mathfrak{B}} \varphi[s] \quad \text{sii} \quad \models_{\mathfrak{B}} \varphi^\pi[s].$$

Éste no es un resultado especialmente fuerte. Solamente dice que φ^π se definió correctamente.

Demostración Usamos inducción sobre φ, aunque solamente en el caso de una fórmula atómica α es no trivial. Para α, usamos inducción sobre el número de lugares en los que ocurren símbolos de función. Es fácil si dicho número es cero. De otra manera,

$$\alpha^\pi = \forall y\,(\pi_g(x, y) \to \beta^\pi),$$

donde $\beta^y_{gx} = \alpha$. (Hemos supuesto, sin decirlo abiertamente, que g es un símbolo de función de un argumento; pero es que la notación ya es bastante mala.) Sea

$$\begin{aligned} b &= \text{la única } b \text{ tal que } \models_{\mathfrak{B}} \pi_g[[s(x), b]] \\ &= g^{\pi\mathfrak{B}}(s(x)). \end{aligned}$$

Entonces

$$\begin{aligned} \models_{\mathfrak{B}} \alpha^\pi[s] &\Leftrightarrow \models_{\mathfrak{B}} \beta^\pi[s(y \mid b)] \\ &\Leftrightarrow \models_{\pi\mathfrak{B}} \beta[s(y \mid b)] && \text{por la hipótesis inductiva} \\ &\Leftrightarrow \models_{\pi\mathfrak{B}} \beta^y_{gx}[s] && \text{por el lema de sustitución} \\ &\Leftrightarrow \models_{\pi\mathfrak{B}} \alpha\,[s]. \end{aligned}$$

⊣

El siguiente corolario justifica nuestra elección de notación para $\pi^{-1}[T_1]$.

Corolario 27C Para un enunciado σ de L_0,

$$\sigma \in \pi^{-1}[T_1] \quad \text{sii} \quad \sigma^\pi \in T_1.$$

Demostración Recuerde que por definición

$$\begin{aligned} \sigma \in \pi^{-1}[T_1] &\Leftrightarrow \text{para todo modelo } \mathfrak{B} \text{ de } T_1, \models_{\pi\mathfrak{B}} \sigma \\ &\Leftrightarrow \text{para todo modelo } \mathfrak{B} \text{ de } T_1, \models_{\mathfrak{B}} \sigma^\pi \\ &\qquad \text{por el Lema 27B} \\ &\Leftrightarrow T_1 \models \sigma^\pi. \end{aligned}$$

⊣

Definición Una *interpretación* π de una teoría T_0 en una teoría T_1 es una interpretación π del lenguaje de T_0 en T_1 tal que

$$T_0 \subseteq \pi^{-1}[T_1].$$

En otras palabras, es necesario que para un enunciado σ de L_0,

$$\sigma \in T_0 \Rightarrow \sigma^\pi \in T_1.$$

$\pi^{-1}[T_1]$ es la teoría más grande que π interpreta en T_1. Si $T_0 = \pi^{-1}[T_1]$, entonces tenemos

$$\sigma \in T_0 \Leftrightarrow \sigma^\pi \in T_1.$$

En este caso se dice que π es una interpretación *fiel* de T_0 en T_1.

Regresando a un ejemplo anterior, consideremos las estructuras $(\mathbb{N}; 0, S)$ y $(\mathbb{Z}; +, \cdot)$. Teníamos entonces una interpretación π en $\mathrm{Th}(\mathbb{Z}; +, \cdot)$, donde

$$\begin{aligned} \pi_\forall(x) &= \exists y_1 \exists y_2 \exists y_3 \exists y_4\, x = y_1 \cdot y_1 + y_2 \cdot y_2 + \\ &\qquad\qquad y_3 \cdot y_3 + y_4 \cdot y_4, \\ \pi_0(x) &= x + x = x, \\ \pi_S(x, y) &= \forall z(z \cdot z = z \wedge z + z \neq z \rightarrow x + z = y). \end{aligned}$$

Ahora afirmamos que π es una interpretación fiel de $\mathrm{Th}(\mathbb{N}; 0, S)$ en $\mathrm{Th}(\mathbb{Z}; +, \cdot)$. Ya que en este caso, ${}^\pi(\mathbb{Z}; +, \cdot)$ *es* la estructura $(\mathbb{N}; 0, S)$. Así que

$$\models_{(\mathbb{N};0,S)} \sigma \iff \models \pi_{(\mathbb{Z};+,\cdot)}\sigma \iff \models_{(\mathbb{Z};+,\cdot)} \sigma^\pi.$$

En el capítulo III podremos demostrar que no hay interpretación de $\mathrm{Th}(\mathbb{Z}; +, \cdot)$ en $\mathrm{Th}(\mathbb{N}; 0, S)$. De modo que la primera teoría es estrictamente más fuerte que la segunda.

Finalmente, regresemos a la situación con la que comenzamos esta sección. Supongamos que T es una teoría que contiene al enunciado ε, donde

$\varepsilon = \forall \mathbf{v}_1 \exists ! \mathbf{v}_2 \varphi$;

$\delta = \forall \mathbf{v}_1, \forall \mathbf{v}_2\ (f \mathbf{v}_1 = \mathbf{v}_2 \leftrightarrow \varphi)$;

L^+ = el lenguaje obtenido al agregar el nuevo símbolo de función f al lenguaje de T;

π = la interpretación de L^+ en T que es la interpretación identidad en todos los parámetros, excepto f, y $\pi_f = \varphi$.

De hecho, π es una interpretación fiel de $\mathrm{Cn}(T;\delta)$ en T, pues, como se había hecho notar antes,

$$\pi^{-1}[T] = \mathrm{Cn}(T;\delta).$$

Ahora podemos sacar una conclusión adicional; la definición *se puede eliminar*.

Teorema 27D Supongamos que se tiene la situación antes descrita. Entonces para cualquier enunciado σ de L^+ podemos encontrar un enunciado σ^π en el lenguaje original, tal que

(a) $T;\delta \models (\sigma \leftrightarrow \sigma^\pi)$.

(b) $T;\delta \models \sigma \iff T \models \sigma^\pi$.

(c) Si f no ocurre en σ, entonces $\models (\sigma \leftrightarrow \sigma^\pi)$.

Demostración La parte (c) se sigue del hecho de que π es la interpretación identidad en todos los parámetros, excepto f. La parte (b) nos dice otra vez que π es una interpretación fiel de $\mathrm{Cn}(T;\delta)$ en T. Como π es fiel, para (a) basta demostrar que

$$T \models (\sigma \leftrightarrow \sigma^\pi)^\pi.$$

Esto se sigue de (c), ya que $(\sigma \leftrightarrow \sigma^\pi)^\pi$ es $(\sigma^\pi \leftrightarrow \sigma^{\pi\pi})$, lo cual es válido. ⊣

Ejercicios

1. Suponga que L_0 y L_1 son lenguajes con los mismos parámetros, excepto que L_0 tiene un símbolo de función f de n argumentos que no está en L_1, y L_1 tiene un símbolo de predicado P de $(n+1)$ argumentos que no está en L_0. Demuestre que para cualquier teoría T de L_0 hay una interpretación fiel de T en alguna teoría de L_1.

2. Sea L_0 el lenguaje con igualdad y los símbolos de función de dos argumentos $+$ y $\cdot$. Sea L_1 lo mismo, pero con símbolos de *predicado* de tres argumentos para suma y producto. Sea $\mathfrak{N}_i = (\mathbb{N}; +, \cdot)$ la estructura para L_i formada por los números naturales con suma y producto

($i = 0, 1$). Demuestre que cualquier relación definible mediante una fórmula de L_0 en $\mathfrak{N}_0$ es también definible por una fórmula de L_1 en $\mathfrak{N}_1$.

3. Demuestre que una interpretación de una teoría completa en una teoría satisfactible es fiel.

8. *Análisis no estándar*[6]

El cálculo diferencial e integral fue descrito originalmente por Leibniz y Newton en el siglo XVII, en términos de cantidades que eran infinitamente pequeñas pero distintas de cero. En sus cálculos, Newton utilizó un número *o* que, siendo infinitamente pequeño, podía ser multiplicado por cualquier número finito y seguía siendo insignificante. Pero era necesario dividir entre *o*, de modo que debería ser diferente de cero. La *dx* de Liebniz era menor que cualquier cantidad asignable, y sin embargo no era cero.

Estas ideas no eran fáciles de comprender ni de aceptar. A lo largo del siglo XVIII se atacó la idea de trabajar con infinitesimales (lo hizo, por ejemplo, el obispo Berkeley), se desconfió de ella (por ejemplo, D'Alembert), y se utilizó en experimentación entusiasta (Euler). Mientras Euler creaba las matemáticas que hoy día se estudian en los cursos de cálculo avanzado, utilizó infinitesimales de una manera muy liberal que no se toleraría hoy en los estudiantes de primer año. No fue sino hasta el siglo XIX cuando se presentaron los fundamentos del cálculo en la forma en que hoy se encuentra en los libros de texto. El tratamiento de los límites fue riguroso y el debate se dejó de lado.

Abraham Robinson introdujo, en 1961, un nuevo método para tratar con los límites, y rescató los infinitesimales del desprestigio intelectual. Este método combina los modernos estándares de rigor con las ventajas intuitivas de trabajar con cantidades infinitamente pequeñas. La idea básica es utilizar un modelo no estándar de la teoría de los números reales.

[6] Esta sección se puede omitir sin que se pierda continuidad.

Construcción de $^*\mathfrak{R}$

Usaremos un lenguaje de primer orden muy grande. Además de los símbolos para $+$, $\cdot$ y $<$, podríamos también agregar símbolos para las funciones exponenciación y valor absoluto. Y como no hay una buena razón para detenernos ahí, pues incluyamos un símbolo para *cada* operación en el conjunto $\mathbb{R}$ de los reales. Hacemos lo mismo para cada relación sobre $\mathbb{R}$. Así, tenemos un lenguaje con igualdad y los parámetros siguientes:

0. $\forall$, que significa "para todos los números reales".

1. Un símbolo de predicado de n argumentos $\mathbf{P}_R$ para cada relación n-aria R sobre $\mathbb{R}$.

2. Un símbolo de constante $\mathbf{c}_r$ para cada $r \in \mathbb{R}$.

3. Un símbolo de función $\mathbf{f}_F$ de n argumentos, para cada operación n-aria F sobre $\mathbb{R}$.

Para este lenguaje hay una estructura estándar $\mathfrak{R}$, con $|\mathfrak{R}| = \mathbb{R}$, $\mathbf{P}_R^{\mathfrak{R}} = R$, $\mathbf{c}_r^{\mathfrak{R}} = r$ y $\mathbf{f}_F^{\mathfrak{R}} = F$. Pero ahora construyamos una estructura no estándar usando el teorema de compacidad. Sea Γ el conjunto

$$\mathrm{Th}\,\mathfrak{R} \cup \{\mathbf{c}_r \mathbf{P}_< \mathbf{v}_1 \mid r \in \mathbb{R}\}.$$

(En este caso, $\mathbf{c}_r \mathbf{P}_< \mathbf{v}_1$ formaliza "r es menor que $\mathbf{v}_1$".) Cualquier subconjunto finito de Γ puede ser satisfecho en $\mathfrak{R}$ si se asigna a $\mathbf{v}_1$ algún número real suficientemente grande. De manera que, por el teorema de compacidad, hay una estructura $\mathfrak{A}$ y un elemento $a \in |\mathfrak{A}|$ tal que Γ se satisface en $\mathfrak{A}$ cuando a $\mathbf{v}_1$ se le asigna a. Como $\mathfrak{A}$ es un modelo de $\mathrm{Th}\,\mathfrak{R}$, tenemos que $\mathfrak{A} \equiv \mathfrak{R}$. También hay un isomorfismo h (aunque no suprayectivo) de $\mathfrak{R}$ en $\mathfrak{A}$, definido como:

$$h(r) = \mathbf{c}_r^{\mathfrak{A}}.$$

Para verificar que h es de verdad un isomorfismo, usamos el hecho de que $\mathfrak{A} \equiv \mathfrak{R}$. h es inyectiva, ya que dados $r_1 \neq r_2$, el enunciado $\mathbf{c}_{r_1} \neq \mathbf{c}_{r_2}$ es verdadero en $\mathfrak{R}$ y, por tanto, en $\mathfrak{A}$. h preserva cualquier relación binaria $R (= \mathbf{P}_R^{\mathfrak{R}})$, ya que para cualesquiera r y s en $\mathbb{R}$,

$$\begin{aligned}\langle r,s\rangle \in P_R^{\mathfrak{R}} &\Leftrightarrow \models_{\mathfrak{R}} P_R c_r c_s\\ &\Leftrightarrow \models_{\mathfrak{A}} P_R c_r c_s\\ &\Leftrightarrow \langle c_r^{\mathfrak{A}}, c_s^{\mathfrak{A}}\rangle \in P_R^{\mathfrak{A}}\\ &\Leftrightarrow \langle h(r), h(s)\rangle \in P_R^{\mathfrak{A}}.\end{aligned}$$

Para cualquier relación n-aria se da un argumento similar. En seguida demostramos que h preserva cualquier función $F(= f_F^{\mathfrak{R}})$. Para simplificar la notación, supondremos, una vez más, que F es una operación binaria. Sean r y s cualesquiera dos elementos de $\mathbb{R}$ y sea $t = F(r,s)$. Entonces

$$\begin{aligned}h(f_F^{\mathfrak{R}}(r,s)) &= h\,(F(r,s))\\ &= h\,(t)\\ &= c_t^{\mathfrak{A}}.\end{aligned}$$

Ahora bien, el enunciado $c_t = f_F c_r c_s$ es verdadero en $\mathfrak{R}$ y, por lo tanto, en $\mathfrak{A}$. Entonces

$$\begin{aligned}c_t^{\mathfrak{A}} &= f_F^{\mathfrak{A}}(c_r^{\mathfrak{A}}, c_s^{\mathfrak{A}})\\ &= f_F^{\mathfrak{A}}(h\,(r), h\,(s)).\end{aligned}$$

De modo que h preserva a f_F. Para los símbolos de constante tenemos por la definición de h,

$$\begin{aligned}h\,(c_r^{\mathfrak{R}}) &= h\,(r)\\ &= c_r^{\mathfrak{A}}.\end{aligned}$$

Como tenemos una copia isomorfa de $\mathfrak{R}$ dentro de $\mathfrak{A}$, podemos encontrar otra estructura $^*\mathfrak{R}$ isomorfa a $\mathfrak{A}$ tal que $\mathfrak{R}$ sea una subestructura de $^*\mathfrak{R}$. La idea es simplemente reemplazar en $\mathfrak{A}$ cada punto $c_r^{\mathfrak{A}}$ por el punto r (suponiendo que $|\mathfrak{A}|\cap\mathbb{R} = \emptyset$, lo que siempre se puede arreglar). Para los detalles, vea el ejercicio 24 de la sección 2 de este capítulo. Como $^*\mathfrak{R}$ es isomorfo a $\mathfrak{A}$, hay un punto $b \in |^*\mathfrak{R}|$ tal que $^*\mathfrak{R}$ satisface Γ cuando a v_1 se le asigna b. En particular, $^*\mathfrak{R} \equiv \mathfrak{R}$.

Para poder avanzar mejor, necesitamos una notación más fácil de manejar. Utilizaremos un asterisco para indicar el paso de $\mathfrak{R}$ a $^*\mathfrak{R}$.

1. Para toda relación n-aria R sobre $\mathbb{R}$, sea $^*R$ la relación $P_R^{^*\mathfrak{R}}$ asignada por $^*\mathfrak{R}$ al símbolo P_R. En particular, $\mathbb{R}$ es una relación

unaria sobre $\mathbb{R}$. Su imagen $^*\mathbb{R}$ es igual al universo de $^*\mathfrak{R}$, ya que el enunciado $\forall x\ P_{\mathbb{R}}x$ es verdadero en $\mathfrak{R}$ y, por lo tanto, en $^*\mathfrak{R}$. Como $\mathfrak{R}$ es una subestructura de $^*\mathfrak{R}$, tenemos que toda relación R es igual a la restricción de $^*R$ a $\mathbb{R}$.

2. Para toda operación n-aria F sobre $\mathbb{R}$, sea $^*F$ la operación $f_R^{*\mathfrak{R}}$ asignada al símbolo f_F por $^*\mathfrak{R}$. Entonces F es la restricción de $^*F$ a $\mathbb{R}$.

Nótese que $c_r^{*\mathfrak{R}} = r$, así que no necesitamos notación especial para este caso.

Hay un método general (que se utilizará ampliamente en el resto de esta sección) para demostrar las propiedades de una relación $^*R$ o una operación $^*F$. Basta observar (1) que R o F tiene la propiedad, (2) que la propiedad puede expresarse mediante un enunciado del lenguaje, y (3) que $\mathfrak{R} \equiv {}^*\mathfrak{R}$.

Por ejemplo, la relación binaria $^*<$ en $^*\mathbb{R}$ es transitiva. Esto se debe a que $<$ es transitiva, y esta propiedad se puede expresar mediante el enunciado

$$\forall x\, \forall y\, \forall z\, (x P_< y \rightarrow y P_< z \rightarrow x P_< z).$$

Con un razonamiento similar se puede ver que $^*<$ satisface la tricotomía en $^*\mathbb{R}$, así que es una relación de orden sobre $^*\mathbb{R}$.

Para dar otro ejemplo; podemos probar que la operación binaria $^*+$ en $^*\mathbb{R}$ es conmutativa, puesto que $+$ es conmutativa y la ley conmutativa se puede expresar mediante un enunciado. Con la aplicación de este razonamiento a cada uno de los axiomas de campo, vemos que $(^*\mathbb{R}; 0, 1, ^*+, ^*\cdot)$ es un campo.

Este método general se utiliza bastante, así que a partir de ahora lo daremos por supuesto. Si, por ejemplo, afirmamos que $^*|a\ ^*+\ b|\ ^*\leq\ ^*|a|\ ^*+\ ^*|b|$ para a y b en $^*\mathbb{R}$, daremos por sentado que el lector se da cuenta de que detrás de este hecho está el método general antes mencionado.

Tenemos $\mathbb{R} \subseteq {}^*\mathbb{R}$, pero $\mathbb{R} \neq {}^*\mathbb{R}$. Ya que tenemos algún elemento b tal que $\models_{^*\mathfrak{R}} c_r P_< v_1[[b]]$; es decir, $r\ ^*<\ b$. Entonces b es infinitamente grande, pues es más grande (en el orden $^*<$) que cualquier elemento estándar r, es decir, que cualquier $r \in \mathbb{R}$. Su recíproco $1\ ^*/\ b$ será un infinitesimal.

Generalmente, las propiedades de $\mathfrak{R}$ que *no pueden* expresarse en el lenguaje son falsas en $^*\mathfrak{R}$. La propiedad de la mí-

nima cota superior es una de ellas. Hay subconjuntos S de $^*\mathbb{R}$ no vacíos que no tienen mínima cota superior (con respecto al orden $^*<$). Por ejemplo, $\mathbb{R}$ es uno de esos subconjuntos de $^*\mathbb{R}$. Está acotado por el punto infinito b del párrafo anterior, pero no tiene mínima cota superior; véase el ejercicio 7.

Definamos el conjunto $\mathcal{F}$ de elementos *finitos* mediante la ecuación

$$\mathcal{F} = \{x \in^* \mathbb{R} \mid {}^*|x| \,{}^*\!< y \quad \text{para algún} \quad y \in \mathbb{R}\}.$$

De manera similar, definamos el conjunto $\mathcal{I}$ de *infinitesimales* mediante la ecuación

$$\mathcal{I} = \{x \in {}^*\mathbb{R} \mid {}^*|x| \,{}^*\!< y \quad \text{para todo } y \text{ positivo, } y \in \mathbb{R}\}.$$

Si $A \subseteq \mathbb{R}$ no está acotado, entonces $^*A$ contiene puntos infinitos. Pues el enunciado "para cualquier real r hay un elemento $a \in A$ más grande que r" es verdadero y formalizable en el lenguaje. Tome algún infinito positivo b; deberá haber un elemento más grande (y por lo tanto infinito) de $^*A$. Por ejemplo, $^*\mathbb{N}$ contiene números infinitos.

El único infinitesimal estándar, es decir, el único elemento de $\mathbb{R} \cap \mathcal{I}$, es 0. Pero hay otros infinitesimales, ya que, por las reglas usuales (formalizables) para las desigualdades, el recíproco de cualquier número infinito es un infinitesimal.

Propiedades algebraicas

En el siguiente teorema se establecen algunos resultados algebraicos sobre $\mathcal{F}$ e $\mathcal{I}$ que serán útiles más adelante.

Teorema 28A (a) $\mathcal{F}$ es cerrado bajo suma $^*+$, resta $^*-$ y producto $^*\cdot$.

(b) $\mathcal{I}$ es cerrado bajo suma $^*+$, resta $^*-$, y producto por elementos de $\mathcal{F}$:

$$x \in \mathcal{I} \quad \text{y} \quad z \in \mathcal{F} \Rightarrow x \,{}^*\!\cdot z \in \mathcal{I}.$$

En terminología algebraica, la parte (a) dice que $\mathcal{F}$ es un subanillo del campo $^*\mathbb{R}$, y la parte (b) dice que $\mathcal{I}$ es un ideal en el anillo $\mathcal{F}$. Un poco más adelante veremos qué es el anillo cociente $\mathcal{F}/\mathcal{I}$.

Demostración (a) Sean x y y finitos, tales que ${}^*|x|\,{}^*\!< a$, ${}^*|y|\,{}^*\!< b$ con a y b elementos estándar en $\mathbb{R}$. Entonces

$${}^*|x \,{}^*\!\pm y|\,{}^*\!\leq {}^*|x|\,{}^*\!+ {}^*|y|\,{}^*\!< a + b \in \mathbb{R},$$

de modo que $x\,{}^*\!+ y$, $x\,{}^*\!- y$ son finitos. También

$${}^*|x\,{}^*\!\cdot y|\,{}^*\!< a \cdot b \in \mathbb{R},$$

así que $x\,{}^*\!\cdot y$ también es finito.

(b) Sean x y y infinitesimales. Entonces dado cualquier elemento estándar positivo a, ${}^*|x|\,{}^*\!< a/2$ y ${}^*|y|\,{}^*\!< a/2$. De modo que

$${}^*|x\,{}^*\!\pm y|\,{}^*\!< a/2 + a/2 = a,$$

así que $x\,{}^*\!+ y$, $x\,{}^*\!- y$ son infinitesimales. Si z es finito, entonces ${}^*|z|\,{}^*\!< b$ para algún estándar b. Como x es infinitesimal, tenemos que ${}^*|x|\,{}^*\!< a/b$, de modo que

$${}^*|x\,{}^*\!\cdot z|\,{}^*\!< (a/b)b = a.$$

Así que $x\,{}^*\!\cdot z$ es también infinitesimal. ⊣

Definición x está *infinitamente cerca* de y (se escribe $x \simeq y$) sii $x\,{}^*\!- y$ es infinitesimal.

Teorema 28B (a) $\simeq$ es una relación de equivalencia sobre ${}^*\mathbb{R}$.

(b) Si $u \simeq v$ y $x \simeq y$, entonces $u\,{}^*\!+ x \simeq v\,{}^*\!+ y$ y ${}^*\!-u \simeq {}^*\!-v$.

(c) Si $u \simeq v$ y $x \simeq y$ y x, y, u, v son finitos, entonces $u\,{}^*\!\cdot x \simeq v\,{}^*\!\cdot y$.

Demostración Ésta es una consecuencia de la parte (b) del teorema anterior ($\mathcal{I}$ es un ideal en $\mathcal{F}$).

(a) $\simeq$ es reflexiva ya que 0 es infinitesimal. $\simeq$ es simétrica puesto que el negativo (${}^*\!-$) de un infinitesimal es infinitesimal. Finalmente, supongamos que $x \simeq y$ y $y \simeq z$. Entonces

$$x\,{}^*\!- z = (x\,{}^*\!- y)\,{}^*\!+ (y\,{}^*\!- z) \in \mathcal{I}$$

ya que $\mathcal{I}$ es cerrado bajo la suma.

(b) Si $u \simeq v$ y $x \simeq y$, entonces

$$(u \mathbin{^*\!+} x) \mathbin{^*\!-} (v \mathbin{^*\!+} y) = (u \mathbin{^*\!-} v) \mathbin{^*\!+} (x \mathbin{^*\!-} y) \in \mathcal{I}$$

dado que $\mathcal{I}$ es cerrado bajo la suma. También $\mathbin{^*\!-} u \simeq \mathbin{^*\!-} v$ ya que $\mathcal{I}$ es cerrado bajo la negación.

(c) $$(u \mathbin{^*\!\cdot} x) \mathbin{^*\!-} (v \mathbin{^*\!\cdot} y) = (u \mathbin{^*\!\cdot} x) \mathbin{^*\!-} (u \mathbin{^*\!\cdot} y) \mathbin{^*\!+} (u \mathbin{^*\!\cdot} y) \mathbin{^*\!-} (v \mathbin{^*\!\cdot} y)$$
$$= u \mathbin{^*\!\cdot} (x \mathbin{^*\!-} y) \mathbin{^*\!+} (u \mathbin{^*\!-} v) \mathbin{^*\!\cdot} y \in \mathcal{I}$$

ya que $\mathcal{I}$ es cerrado bajo el producto por elementos de $\mathcal{F}$. ⊣

Dados r y s estándar, tenemos que $r \simeq s$ sii $r = s$, ya que 0 es el único infinitesimal estándar.

Lema 28C Si $x \not\simeq y$ y al menos uno es finito, entonces hay un punto estándar q que está estrictamente entre x y y.

Demostración Supondremos que $x \mathbin{^*\!<} y$. De hecho, podemos ir más lejos y suponer que $0 \mathbin{^*\!<} x \mathbin{^*\!<} y$; el caso $x \mathbin{^*\!<} y \mathbin{^*\!\leq} 0$ es similar, y el caso $x \mathbin{^*\!<} 0 \mathbin{^*\!<} y$ es trivial. Como $x \not\simeq y$, entonces hay un punto estándar b tal que $0 < b \mathbin{^*\!<} y \mathbin{^*\!-} x$. Como x es finito, tenemos $x \mathbin{^*\!<} mb$ para algún entero positivo m; tomemos la mínima m que cumpla eso. Entonces $x \mathbin{^*\!<} mb \mathbin{^*\!<} y$. (Por la minimalidad de m, $(m-1)b \mathbin{^*\!\leq} x$; así que $mb \mathbin{^*\!\leq} x \mathbin{^*\!+} b \mathbin{^*\!<} y$.) ⊣

Teorema 28D Todo $x \in \mathcal{F}$ es infinitamente cercano a un único $r \in \mathbb{R}$.

Demostración Dado $x \in \mathcal{F}$, el conjunto

$$S = \{y \in \mathbb{R} \mid y \mathbin{^*\!<} x\}$$

de puntos estándar menores que x tiene una cota superior en $\mathbb{R}$. Sea r su mínima cota superior; afirmamos que $x \simeq r$.

Si $x \not\simeq r$, entonces, por el lema hay un estándar q entre x y r. Si $r < q \mathbin{^*\!<} x$, entonces r no sería cota superior de S. Si $x \mathbin{^*\!<} q < r$, entonces q sería también cota superior de S, lo cual contradice la minimalidad de r. Por lo tanto, $x \simeq r$.

Esto establece la existencia de r. En cuanto a la unicidad, obsérvese que si $x \simeq r$ y $x \simeq s$, entonces $r \simeq s$. Para puntos estándar r y s, eso implica que $r = s$. ⊣

Corolario 28E Todo x finito tiene una descomposición única de la forma $x = s \,{}^*\!+ i$, donde s es estándar e i es infinitesimal.

Llamamos a s la *parte estándar* de x, denotada por $\mathrm{st}(x)$. (Otra notación para la parte estándar de x es ${}^\circ x$.) Por supuesto, para un punto estándar r, $\mathrm{st}(r) = r$. El siguiente teorema resume algunas propiedades de la función st.

Teorema 28F (a) st es una función de $\mathcal{F}$ sobre $\mathbb{R}$.

(b) $\mathrm{st}(x) = 0$ sii x es infinitesimal.

(c) $\mathrm{st}(x \,{}^*\!+ y) = \mathrm{st}(x) + \mathrm{st}(y)$.

(d) $\mathrm{st}(x \,{}^*\!\cdot y) = \mathrm{st}(x) \cdot \mathrm{st}(y)$.

Demostración Las partes (a) y (b) son claras. Como $\mathrm{st}(x) \simeq x$ y $\mathrm{st}(y) \simeq y$, tenemos, por la parte (b) del teorema 28B, que $\mathrm{st}(x) + \mathrm{st}(y) \simeq x \,{}^*\!+ y$. Por tanto, el lado izquierdo es igual a $\mathrm{st}(x \,{}^*\!+ y)$. La parte (d) es similar y usa la parte (c) del teorema 28B.

(En términos algebraicos, este teorema afirma que st es un homomorfismo del anillo $\mathcal{F}$ sobre el campo $\mathbb{R}$, con núcleo $\mathcal{I}$. En consecuencia, el anillo cociente $\mathcal{F}/\mathcal{I}$ es isomorfo al campo real $\mathbb{R}$.)

En lo que sigue de esta sección, para hacer más fluida la notación omitiremos los asteriscos en los símbolos para las operaciones aritméticas ${}^*\!+$, ${}^*\!-$, ${}^*\!\cdot$ y ${}^*\!/$.

Convergencia

En los cursos de cálculo normalmente se trata la convergencia en términos de ε y δ y variables que se acercan bastante a ciertos valores. Aquí presentaremos el principio de una forma alternativa de abordar la convergencia, donde las variables llegan a ser infinitamente cercanas a los valores límites.

Definición Sea $F : \mathbb{R} \to \mathbb{R}$. Entonces F *converge en* a a b sii siempre que x esté infinitamente cercana a a (pero

sea diferente de a), entonces $^*F(x)$ está infinitamente cercana a b.

Demostración de la equivalencia con la definición ordinaria Primero supongamos que F converge en a a b en el sentido ordinario. Esto es, para cualquier $\varepsilon > 0$ hay una $\delta > 0$ tal que

$$0 \neq |x - a| < \delta \Rightarrow |b - F(x)| < \varepsilon \quad \text{para cualquier } x.$$

El enunciado mostrado (respecto de los números estándar ε y δ) es formalizable y, por tanto, se cumple en $^*\mathfrak{R}$. Ahora bien, si x en $^*\mathbb{R}$ está infinitamente cercana a a (pero es diferente de a), entonces ciertamente $0 \neq {}^*|x - a| \;{}^*\!< \delta$. Por lo tanto, $^*|b - {}^*F(x)| \;{}^*\!< \varepsilon$. Como ε era arbitraria, $b \simeq {}^*F(x)$.

Inversamente, supongamos que se cumple la condición establecida en la definición. Entonces, para cualquier $\varepsilon > 0$ estándar, el enunciado

$$\text{Existe } \delta > 0 \text{ tal que para toda } x, 0 \neq |a-x| < \delta \Rightarrow |b-F(x)| < \varepsilon$$

(una vez formalizado) es verdadero en $^*\mathfrak{R}$, ya que podemos tomar una δ infinitesimal. Por lo tanto el enunciado también es verdadero en $\mathfrak{R}$. ⊣

Primer comentario: Es completamente posible que, en a, F no converja a ningún número. Por otra parte, F converge en a cuando mucho a una b, porque si i es un infinitesimal diferente de cero, entonces $b = \text{st}\,({}^*F(a + i))$. Tradicionalmente, esta b se denota con "$\lim_{x\to a} F(x)$". De modo que

$$\lim_{x\to a} F(x) = \text{st}({}^*F(a + i)).$$

Segundo comentario: En realidad no es necesario tener $\text{dom}\, F = \mathbb{R}$. Es suficiente con que a sea un punto de acumulación de $\text{dom} F$ (a es un punto de acumulación de S sii a está infinitamente cercano a algún elemento de $^*S$, pero es diferente de él).

Corolario 28G F es continua en a sii siempre que $x \simeq a$, entonces $^*F(x) \simeq F(a)$.

Ahora consideremos una función $F : \mathbb{R} \to \mathbb{R}$ y un punto estándar $a \in \mathbb{R}$. Entonces, la derivada $F'(a)$ es

$$\lim_{h \to 0} \frac{F(a+h) - F(a)}{h}.$$

Gracias a nuestra definición de límite, esto también se puede expresar como: $F'(a) = b$ sii para todo infinitesimal dx diferente de cero tenemos que $dF/dx \simeq b$, donde $dF = {}^*F(a + dx) - F(a)$. Así, si hay tal b (es decir, si $F'(a)$ existe), entonces

$$F'(a) = \operatorname{st}(dF/dx)$$

para cualquier infinitesimal dx diferente de cero. En este caso, dF/dx es el resultado de *dividir* dF entre dx. El hecho de que aquí solamente usemos la división facilita mucho los cálculos.

Ejemplo Sea $F(x) = x^2$. Entonces, $F'(a) = 2a$, ya que

$$\frac{dF}{dx} = \frac{(a + dx)^2 - a^2}{dx} = \frac{2a(dx) + (dx)^2}{dx} = 2a + dx \simeq 2a.$$

Teorema 28H Si $F'(a)$ existe, entonces F es continua en a.

Demostración Para cualquier infinitesimal dx diferente de cero tenemos

$$\frac{{}^*F(a + dx) - F(a)}{dx} \simeq F'(a).$$

El lado derecho es estándar, así que el lado izquierdo es por lo menos finito. En consecuencia, cuando multiplicamos el lado izquierdo por el infinitesimal dx, nos quedamos con el resultado de que ${}^*F(a + dx) - F(a) \in \mathcal{I}$; es decir, ${}^*F(a + dx) \simeq F(a)$. ⊣

El lector debe observar que este resultado no es una versión no estándar de un teorema clásico, ni tampoco una generalización de un teorema clásico. En realidad *es* un teorema clásico. Lo que no es estándar es solamente la demostración. Lo mismo podemos decir del siguiente teorema. Sea $F \circ G$ la función cuyo valor en a es $F(G(a))$.

Regla de la cadena Supongamos que $G'(a)$ y $F'(G(a))$ existen. Entonces $(F \circ G)'(a)$ existe y es igual a $F'(G(a)) \cdot G'(a)$.

Demostración Primero, obsérvese que $^*(F \circ G) = {}^*F \circ {}^*G$, ya que el enunciado $\forall v_1\, f_{F \circ G} v_1 = f_F f_G v_1$ es verdadero en las estructuras. Ahora, considere cualquier infinitesimal dx diferente de cero. Sea

$$\begin{aligned} dG &= {}^*G(a + dx) - G(a), \\ dF &= {}^*(F \circ G)(a + dx) - (F \circ G)(a) \\ &= {}^*F({}^*G(a + dx)) - F(G(a)) \\ &= {}^*F(G(a) + dG) - F(G(a)). \end{aligned}$$

Entonces, $dG \simeq 0$, ya que G es continua en a. Si $dG \neq 0$, entonces, por la última de estas ecuaciones, $dF/dG \simeq F'(G(a))$, de modo que

$$\frac{dF}{dx} = \frac{dF}{dG} \cdot \frac{dG}{dx} \simeq F'(G(a)) \cdot G'(a).$$

Si $dG = 0$, entonces $dF = 0$ y $G'(a) \simeq dG/dx = 0$, así que de nuevo tenemos

$$\frac{dF}{dx} \simeq F'(G(a)) \cdot G'(a).$$

⊣

Estos teoremas no son más que ejemplos del tratamiento de la convergencia en términos de la proximidad infinita. El método de ninguna manera se limita a temas básicos. Podemos construir funciones delta δ, con la propiedad de que $\int_{-\infty}^{\infty} \delta = 1$; y, sin embargo, $\delta(x) \simeq 0$ para $x \not\simeq 0$. Se han obtenido resultados originales en análisis (por ejemplo, en la teoría de los espacios de Hilbert) mediante el método de análisis no estándar. Posiblemente en el futuro se llegue a generalizar el uso del método cuando más analistas se familiaricen con él.

Ejercicios

1. ($\mathbb{Q}$ es denso en $\mathbb{R}$.) Sea $\mathbb{Q}$ el conjunto de los números racionales. Muestre que cada elemento de $^*\mathbb{R}$ está infinitamente cercano a algún elemento de $^*\mathbb{Q}$.

2. (a) Sea $A \subseteq \mathbb{R}$ y $F : A \to \mathbb{R}$. Entonces F también es una relación binaria sobre $\mathbb{R}$; muestre que ${}^*F : {}^*A \to {}^*\mathbb{R}$.
   (b) Sea S: $\mathbb{N} \to \mathbb{R}$. Recuerde que se dice que S converge a b sii para toda $\varepsilon > 0$ hay algún k tal que para todo $n > k$, $|S(n) - b| < \varepsilon$. Muestre que esto es equivalente a la condición: ${}^*S(x) \simeq b$ para todo $x \in {}^*\mathbb{N}$, con x infinito.
   (c) Suponga que $S_i : \mathbb{N} \to \mathbb{R}$ y S_i converge a b_i para $i = 1, 2$. Demuestre que $S_1 + S_2$ converge a $b_1 + b_2$ y $S_1 \cdot S_2$ converge a $b_1 \cdot b_2$.

3. Sea $F : A \to \mathbb{R}$ uno a uno, donde $A \subseteq \mathbb{R}$. Demuestre que si $x \in {}^*A$ pero $x \notin A$, entonces ${}^*F(x) \notin \mathbb{R}$.

4. Sea $A \subseteq \mathbb{R}$. Muestre que $A = {}^*A$ sii A es finito.

5. (Teorema de Bolzano-Weierstrass) Sea $A \subseteq \mathbb{R}$ acotado e infinito. Demuestre que hay un punto $p \in \mathbb{R}$ que está infinitamente cercano pero es diferente de algún elemento de ${}^*A$. *Sugerencia:* Sea $S : \mathbb{N} \to A$ con S uno a uno; fíjese en ${}^*S(x)$ para $x \in {}^*\mathbb{N}$, con x infinito.

6. (a) Demuestre que ${}^*\mathbb{Q}$ tiene cardinalidad al menos de $2^{\aleph_0}$, donde $\mathbb{Q}$ es el conjunto de los números racionales. *Sugerencia:* Use el ejercicio 1.
   (b) Demuestre que ${}^*\mathbb{N}$ tiene cardinalidad al menos de $2^{\aleph_0}$.

7. Sea A un subconjunto de $\mathbb{R}$ sin elemento máximo. Entonces, como subconjunto de ${}^*\mathbb{R}$, A tendrá cotas superiores (con respecto al orden ${}^*<$) en ${}^*\mathbb{R}$. Pero demuestre que A no tiene mínima cota superior.

III

INDECIDIBILIDAD

0. *Teoría de números*

En este capítulo nos concentraremos en el estudio de un lenguaje específico: el lenguaje de la teoría de números. Éste será un lenguaje de primer orden con igualdad y con los siguientes parámetros:

$\forall$, cuyo significado será "para todo número natural". (Recuérdese que el conjunto $\mathbb{N}$ de los números naturales es $\{0, 1, 2, \ldots\}$. El cero es considerado número natural.)

0, un símbolo de constante que denotará al número 0.

S, un símbolo de función de una variable, que denotará la función sucesor $S : \mathbb{N} \to \mathbb{N}$; es decir, la función por la que $S(n) = n + 1$.

$<$, un símbolo de predicado binario que denotará la relación de orden usual (estricto) de $\mathbb{N}$.

$+$, $\cdot$, **E**, símbolos de función de dos variables que denotarán las operaciones $+$, $\cdot$ y E de suma, producto y exponenciación, respectivamente.

Llamaremos $\mathfrak{N}$ a la estructura propuesta para este lenguaje, que podemos escribir informalmente como:

$$\mathfrak{N} = (\mathbb{N}; 0, S, <, +, \cdot, E)$$

(Donde $|\mathfrak{N}| = \mathbb{N}$, $\mathbf{0}^{\mathfrak{N}} = 0$, etcétera.)

Por ***teoría de números*** entendemos la teoría de esta estructura, $\text{Th}\,\mathfrak{N}$. A manera de preparación estudiaremos (en las secciones 1 y 2 de este capítulo) algunos reductos particulares de $\mathfrak{N}$; es decir, las restricciones de $\mathfrak{N}$ para los sublenguajes:

$$\begin{aligned}\mathfrak{N}_S &= (\mathbb{N}; 0, S),\\ \mathfrak{N}_L &= (\mathbb{N}; 0, S, <),\\ \mathfrak{N}_A &= (\mathbb{N}; 0, S, <, +).\end{aligned}$$

Finalmente, en la sección 8 de este capítulo consideraremos

$$\mathfrak{N}_M = (\mathbb{N}, 0, S, <, +, \cdot).$$

Nos plantearemos las mismas preguntas respecto de cada una de estas estructuras:

(A) ¿Es decidible la teoría de la estructura? Si lo es, ¿cuál puede ser un conjunto adecuado de axiomas para la teoría? ¿Hay un conjunto finito de axiomas?

(B) ¿Qué subconjuntos de $\mathbb{N}$ son definibles en la estructura?

(C) ¿Cómo son los modelos no estándar de la teoría de la estructura? (Por "no estándar" entendemos que "no sean isomorfos a la estructura propuesta".)

La razón por la que elegimos estudiar la teoría de números (en lugar, por ejemplo, de la teoría de grupos) es la siguiente: podemos demostrar que una subteoría particular de la teoría de números es un conjunto indecidible de enunciados. También vamos a poder concluir que cualquier teoría que sea al menos tan fuerte como este fragmento de la teoría de números (por ejemplo, la teoría de números o la teoría de conjuntos en su totalidad) debe ser indecidible. Esto quiere decir, en particular, que dicha teoría no puede ser al mismo tiempo completa y axiomatizable.

Para demostrar que nuestra subteoría de la teoría de números es indecidible, mostraremos que ésta es lo suficientemente fuerte como para representar (en un sentido que será precisado más adelante) resultados sobre sucesiones de números, sobre ciertas operaciones entre números y, finalmente, sobre procedimientos de decisión. Esta característica de la subteoría nos permitirá utilizar un argumento diagonal para demostrar la indecidibilidad.

Cabe hacer notar que, en lugar de una subteoría de la teoría de números, podríamos utilizar cualquier otra teoría (como algún fragmento de la teoría de conjuntos finitos) en la que se

puedan representar de forma adecuada resultados de los procedimientos de decisión.

Antes de presentar ejemplos que den cuenta de la riqueza expresiva del lenguaje de la teoría de números, sería conveniente introducir algunas convenciones sobre la notación. Escribiremos, como concesión al uso cotidiano:

$$x < y, \quad x + y, \quad x \cdot y \quad \text{y} \quad x \mathbf{E} y$$

en lugar de su expresión formal

$$< xy, \quad + xy, \quad \cdot xy \quad \text{y} \quad \mathbf{E}\, xy.$$

Para todo número natural k, tendremos un término $\mathbf{S}^k\mathbf{0}$ (el *numeral* de k) que lo denota:

$$\mathbf{S}^0\mathbf{0} = \mathbf{0}, \quad \mathbf{S}^1\mathbf{0} = \mathbf{S0}, \quad \mathbf{S}^2\mathbf{0} = \mathbf{SS0}, \quad \text{etc.}$$

(El conjunto de los numerales se genera a partir de $\{\mathbf{0}\}$ mediante la operación de anteponer **S**.) El hecho de que todo número natural pueda ser nombrado con el lenguaje será de gran utilidad.

A pesar de que sólo hay una cantidad numerable de relaciones sobre $\mathbb{N}$ que pueden ser definidas en $\mathfrak{N}$, casi todas las relaciones conocidas pueden ser definidas en $\mathfrak{N}$. Por ejemplo, el conjunto de los primos está definido en $\mathfrak{N}$ por

$$v_1 \neq \mathbf{S}^1\mathbf{0} \wedge \forall v_2\, \forall v_3(v_1 = v_2 \cdot v_3 \rightarrow v_2 = \mathbf{S}^1\mathbf{0} \vee v_3 = \mathbf{S}^1\mathbf{0}).$$

Más adelante necesitaremos probar que muchas otras relaciones particulares son definibles en $\mathfrak{N}$.

Resulta natural pensar que, al deshacernos de algún parámetro, se reduce notablemente la capacidad expresiva del lenguaje. Por ejemplo, veremos que el conjunto de los primos no es definible en $\mathfrak{N}_A$. Por otro lado, en la sección 8 demostraremos que cualquier relación definible en $\mathfrak{N}$ también es definible en $\mathfrak{N}_M$.

Preliminares

Los principales teoremas de este capítulo —teoremas asociados con los nombres de Gödel, Tarski y Church— no se demostrarán hasta la sección 5; sin embargo introduciremos desde ahora

algunas de las ideas centrales. Lo que se quiere comparar son las nociones de *verdad* y *prueba*; es decir, se quiere comparar el conjunto de enunciados *verdaderos* en $\mathfrak{N}$ con el conjunto de enunciados que podrían ser *probados* a partir de un conjunto adecuado de axiomas A.

A cada fórmula α del lenguaje de la teoría de números le podemos asignar un número entero $\sharp\alpha$, llamado el número de Gödel de α. Cualquier forma lo suficientemente explícita de asignar enteros distintos a fórmulas distintas nos servirá para nuestros propósitos; al principio de la sección 4 se presentará una asignación particular. Lo importante *es* que para cada α podamos decir qué número $\sharp\alpha$ le corresponde, y viceversa. De manera similar, a cada sucesión D finita de fórmulas (como es el caso de una deducción) le asignamos un entero $\mathcal{G}(D)$. Obsérvese que para cualquier *conjunto* A de fórmulas podemos formar el conjunto de números $\{\sharp\alpha \mid \alpha \in A\}$ correspondiente.

Una vez dada la forma de representación, podemos elegir entre tres formas de argumentación distintas para la demostración: el *argumento de autorreferencia*, el *argumento de diagonalización*, y el *argumento de computabilidad*. Más adelante se mostrará que estos tres argumentos están íntimamente ligados, al menos más de lo que parece (pues en realidad se trata de tres formas particulares de una idea general para la demostración).

En el primer caso, el del *argumento de autorreferencia*, se construye un enunciado σ que nos dice algo así como "No soy demostrable". En realidad, lo que tenemos es lo siguiente:

Teorema 30A Sea $A \subseteq \mathrm{Th}\,\mathfrak{N}$ un conjunto de enunciados verdaderos en $\mathfrak{N}$, y supongamos que el conjunto $\{\sharp\alpha \mid \alpha \in A\}$ de los números de Gödel de los elementos de A es un conjunto definible en $\mathfrak{N}$. Entonces podemos encontrar un enunciado σ tal que es verdadero en $\mathfrak{N}$ pero no es deducible a partir de A.

Demostración Construiremos σ de modo que exprese (indirectamente) que él mismo no es teorema de A. Entonces el argumento será, en términos generales, el siguiente: Si $A \vdash \sigma$, entonces lo que dice σ es falso, contradiciendo el hecho de que A es un conjunto de enunciados verdaderos. Por lo tanto, $A \nvdash \sigma$ y, entonces, σ es verdadero.

Para construir σ, primero consideramos, la siguiente relación ternaria R:

$\langle a, b, c \rangle \in R$ sii a es el número de Gödel para alguna fórmula α y c es el valor de $\mathcal{G}$ para alguna deducción de $\alpha(\mathbf{S}^b\mathbf{0})$ a partir de A.

Ahora bien, como $\{\sharp\alpha \mid \alpha \in A\}$ es definible en $\mathfrak{N}$, entonces R también es definible. (Los detalles de este paso se verán en una sección posterior.) Sea ρ la fórmula que define R en $\mathfrak{N}$. Sea q el número de Gödel de:

$$\forall v_3 \neg \rho(v_1, v_1, v_3).$$

(Aquí utilizamos la notación: $\varphi(t) = \varphi_t^{v_1}$, $\varphi(t_1, t_2) = (\varphi_{t_1}^{v_1})_{t_2}^{v_2}$, y así sucesivamente.) Sea σ:

$$\forall v_3 \neg \rho(\mathbf{S}^q\mathbf{0}, \mathbf{S}^q\mathbf{0}, v_3).$$

Entonces, lo que σ afirma es que no hay un número que sea el valor de $\mathcal{G}$ asignado a una deducción, a partir de A, de la fórmula que resulta de sustituir, en la fórmula con número de Gödel q, la variable v_1 por el numeral q. Lo que, como se verá, implica que no hay un número que sea el valor de $\mathcal{G}$ de una deducción de σ.

Supongamos, contra lo que esperamos, que hay una deducción de σ a partir de A. Sea k el valor asignado por $\mathcal{G}$ a tal deducción. Entonces tenemos que $\langle q, q, k \rangle \in R$ y, por lo tanto:

$$\models_{\mathfrak{N}} \rho(\mathbf{S}^q\mathbf{0}, \mathbf{S}^q\mathbf{0}, \mathbf{S}^k\mathbf{0}).$$

Por otro lado, está claro que

$$\sigma \vdash \neg \rho(\mathbf{S}^q\mathbf{0}, \mathbf{S}^q\mathbf{0}, \mathbf{S}^k\mathbf{0})$$

y a partir de los últimos dos renglones podemos concluir que σ es falso en $\mathfrak{N}$. Pero $A \vdash \sigma$ y los elementos de A son verdaderos en $\mathfrak{N}$, por lo que tenemos una contradicción.

Por lo tanto, no hay una deducción de σ a partir de A. Lo que permite concluir que para todo k tenemos que $\langle q, q, k\rangle \notin R$. Es decir, para todo k

$$\models_{\mathfrak{N}} \neg\rho(\mathbf{S}^q\mathbf{0}, \mathbf{S}^q\mathbf{0}, \mathbf{S}^k\mathbf{0}),$$

de donde se sigue (usando el lema de sustitución) que

$$\models_{\mathfrak{N}} \forall v_3 \neg\rho(\mathbf{S}^q\mathbf{0}, \mathbf{S}^q\mathbf{0}, v_3);$$

es decir, σ es verdadero en $\mathfrak{N}$. ⊣

Más adelante demostraremos —usando algo que se conoce como la *tesis de Church*— que cualquier conjunto decidible de números naturales debe ser definible en $\mathfrak{N}$, a partir de lo cual podremos concluir que Th $\mathfrak{N}$ no es axiomatizable.

Corolario 30B El conjunto $\{\sharp\tau \mid \models_{\mathfrak{N}} \tau\}$ de los números de Gödel de enunciados verdaderos en $\mathfrak{N}$ es un conjunto no definible en $\mathfrak{N}$.

Demostración Si este conjunto fuera definible, entonces podríamos sustituir A por Th $\mathfrak{N}$ en el teorema anterior para llegar a una contradicción. ⊣

En la sección 5 se retomará el *argumento de autorreferencia*, aunque con una pequeña variante en el enunciado σ, el cual afirmará algo así como "soy falso". (¡Recuérdese la conocida paradoja del mentiroso!)

Sin embargo, para quienes tengan la sensación de que el enunciado σ del *argumento de autorreferencia* parece un truco mágico, tenemos *el argumento de diagonalización* que permite describir la situación sin que la autorreferencia sea explícita.

En este caso comenzamos definiendo una relación binaria P entre números naturales:

$\langle a, b\rangle \in P \Longleftrightarrow a$ es el número de Gödel de una fórmula $\alpha(v_1)$ (con v_1 como única variable libre) y $\models_{\mathfrak{N}} \alpha(\mathbf{S}^b\mathbf{0})$.

(Intuitivamente, $\langle a, b\rangle \in P \Leftrightarrow$ "a es verdadera acerca de b".) Entonces, cualquier conjunto de números naturales definible en $\mathfrak{N}$ es igual, para alguna a, a la "sección vertical" de P:

$$P_a = \{b \mid \langle a,b\rangle \in P\}.$$

Esto es, basta considerar que a es igual al número de Gödel de la fórmula que define al conjunto, y usar el hecho de que $\models_{\mathfrak{N}} \alpha(\mathbf{S}^b\mathbf{0}) \Leftrightarrow \models_{\mathfrak{N}} \alpha(v_1)[[b]]$.

De este modo tenemos que todo conjunto de números naturales definible (en $\mathfrak{N}$) está en algún lugar de la lista $P_1, P_2, \ldots$ El siguiente paso será *diagonalizar* esta lista. Definimos el conjunto H como sigue:

$$H = \{b \mid \langle b,b\rangle \notin P\}.$$

(Intuitivamente, $b \in H \Leftrightarrow$ "b no es verdadero acerca de b".) Entonces H no está en la lista $P_1, P_2, \ldots$ ($H \neq P_3$ ya que $3 \in H \Leftrightarrow 3 \notin P_3$. Es decir, el número 3 pertenece sólo a uno de estos conjuntos y no al otro.) Por lo tanto, H no es definible en $\mathfrak{N}$.

¿Por qué es H indefinible? Si incluso se había especificado que

$b \in H \Leftrightarrow$ no [b es el número de Gödel de una fórmula $\alpha(v_1)$ con v_1 como única variable libre y $\models_{\mathfrak{N}} \alpha(\mathbf{S}^b\mathbf{0})$].

¿Qué es lo que impide que esta propiedad sea traducida al lenguaje de la aritmética? Mostraremos que la dificultad *no* está en traducir ser número de Gödel —cosa que se puede hacer—, como tampoco está en que se tenga una fórmula con una variable libre sin que se sustituya por el numeral $\mathbf{S}^b\mathbf{0}$. En realidad, mediante un proceso de eliminación, se mostrará que el único obstáculo que podemos encontrar es que sea imposible decir, mediante el lenguaje de la aritmética, que un enunciado es verdadero en $\mathfrak{N}$.

Teorema 30C (a) El conjunto $\{\sharp\tau \mid \models_{\mathfrak{N}} \tau\}$ de los números de Gödel de enunciados verdaderos en $\mathfrak{N}$ no es definible en $\mathfrak{N}$.

*(b) La teoría Th $\mathfrak{N}$ es indecidible.

*(c) La teoría Th $\mathfrak{N}$ no es axiomatizable.

Demostración Para el inciso (a), que establece lo mismo que el corolario 30B del *argumento de autorreferencia*, se usa

la demostración de la diagonalización que acabamos de exponer; puesto que si suponemos lo contrario, es decir, que Th $\mathfrak{N}$ es definible en $\mathfrak{N}$, entonces el conjunto H también es definible en $\mathfrak{N}$, pero ya vimos que no lo es.

El inciso (b) se deducirá una vez que se demuestre que todo conjunto decidible de números naturales debe ser definible. Si Th $\mathfrak{N}$ es decidible, entonces el conjunto correspondiente de números de Gödel $\{\sharp\tau \mid \models_{\mathfrak{N}} \tau\}$ es decidible y, por lo tanto, definible; lo cual no es cierto.

El inciso (c) es una consecuencia inmediata del inciso (b) y del corolario 26I, pues Th $\mathfrak{N}$ es una teoría completa. ⊣

Por último, tenemos el *argumento de computabilidad* que presenta una diferencia muy clara y precisa entre el conjunto de lo que es verdadero y el conjunto de lo que es demostrable. A partir de la sección 6 del capítulo II sabemos que para cualquier conjunto A decidible de axiomas (incluso si es efectivamente numerable) que elijamos para la Th $\mathfrak{N}$, el conjunto Cn A de enunciados demostrables es un conjunto efectivamente numerable.

El argumento de computabilidad demostrará —utilizando la tesis de Church— que el conjunto Th $\mathfrak{N}$ de todos los enunciados verdaderos *no* es efectivamente numerable. Este resultado, estrechamente ligado al teorema 30C, se obtendrá mediante otro argumento de diagonalización que será presentado en la sección 6 de este capítulo.

***Teorema 30D** Para cualquier conjunto A decidible de axiomas (incluso efectivamente numerable),

$$\mathrm{Cn}\,A \neq \mathrm{Th}\,\mathfrak{N}$$

pues el conjunto de la izquierda es efectivamente numerable y el de la derecha no.

El teorema 30D plantea el siguiente dilema: o los axiomas nos engañan permitiéndonos deducir enunciados falsos, o los axiomas son insuficientes, en el sentido de que existen enunciados verdaderos que no pueden deducirse a partir de esos axiomas.

El argumento de computabilidad aparece de manera implícita en la sección 5 de este capítulo, pero no será sino hasta la sección 6 donde se expondrá formalmente y donde además se le comparará con las otras dos formas de argumentación.

1. *Números naturales con la función sucesor*

Comenzaremos con un caso lo suficientemente sencillo como para poder responder con precisión a nuestras preguntas. Reduciremos el conjunto de parámetros a $\forall$, $\mathbf{0}$ y $\mathbf{S}$, eliminando $<$, $+$, $\cdot$ y $\mathbf{E}$. El reducto correspondiente de $\mathfrak{N}$ es

$$\mathfrak{N}_S = (\mathbb{N}; 0, S).$$

Con esta restricción de lenguaje, es posible nombrar a cada elemento de $\mathbb{N}$, pues en él ya se tienen los numerales. Sin embargo, los enunciados que pueden construirse a partir de este lenguaje no son interesantes desde el punto de vista aritmético.

Nos interesa preguntarnos, sobre $\mathfrak{N}_S$, lo mismo que nos preguntamos para el caso de $\mathfrak{N}$. Quisiéramos saber cuán complejo es el conjunto $\text{Th}\,\mathfrak{N}_S$, investigar cuáles son los conjuntos definibles en $\mathfrak{N}_S$ y tener una idea de sus modelos no estándar.

Para el análisis de la teoría de números naturales con la función sucesor ($\text{Th}\,\mathfrak{N}_S$), comenzaremos listando algunos de sus elementos, es decir, enunciados verdaderos en $\mathfrak{N}_S$. (Después de todo, son estos enunciados los que nos permitirán dar una axiomatización de la teoría.)

S1. $\forall x\, \mathbf{S}x \neq \mathbf{0}$. El cero no tiene predecesor.

S2. $\forall x\, \forall y\, (\mathbf{S}x = \mathbf{S}y \rightarrow x = y)$. La función sucesor es inyectiva.

S3. $\forall y\, (y \neq \mathbf{0} \rightarrow \exists x\; y = \mathbf{S}x)$. Todo número distinto de cero es sucesor de algún número.

S4.1. $\forall x\, \mathbf{S}x \neq x$.

S4.2. $\forall x\, \mathbf{SS}x \neq x$.

...

S4.n $\forall x\, \mathbf{S}^n x \neq x$, donde el superíndice n indica que el símbolo S aparece n veces consecutivas.

Sea A_S el conjunto de enunciados S1, S2, S3 y S4.n (con $n = 1, 2, \ldots$) antes expuestos. Está claro que estos enunciados

son verdaderos en $\mathfrak{N}_S$. Por lo tanto, $\mathfrak{N}_S$ es modelo de A_S y

$$\mathrm{Cn}A_S \subseteq \mathrm{Th}\,\mathfrak{N}_S.$$

(Cualquier cosa que sea verdadera en todos los modelos de A_S es verdadera en $\mathfrak{N}_S$.) Sin embargo, la igualdad no resulta evidente. Para probarla tomaremos un modelo arbitrario de A_S.

¿Qué podemos decir acerca de un modelo arbitrario

$$\mathfrak{A} = (|\mathfrak{A}|; \mathbf{0}^{\mathfrak{A}}, \mathbf{S}^{\mathfrak{A}})$$

del conjunto de axiomas A_S? $\mathbf{S}^{\mathfrak{A}}$ debe ser una función biyectiva de $|\mathfrak{A}|$ sobre $|\mathfrak{A}| - \{\mathbf{0}^{\mathfrak{A}}\}$ por los axiomas S1, S2 y S3, y como el axioma S4 prohíbe la existencia de ciclos de longitud n, entonces $|\mathfrak{A}|$ debe contener los puntos "estándar":

$$\mathbf{0}^{\mathfrak{A}} \to \mathbf{S}^{\mathfrak{A}}(\mathbf{0}^{\mathfrak{A}}) \to \mathbf{S}^{\mathfrak{A}}(\mathbf{S}^{\mathfrak{A}}(\mathbf{0}^{\mathfrak{A}})) \to \ldots,$$

que son todos distintos. La flecha indica la aplicación de la función $\mathbf{S}^{\mathfrak{A}}$. Puede o no haber otros elementos en $|\mathfrak{A}|$. Supongamos que hay otro elemento a en $|\mathfrak{A}|$, no "estándar", entonces también está el sucesor de a, y el sucesor del sucesor, etc. Más aún, puesto que (por S3) todo elemento distinto del cero tiene un predecesor (es decir, es sucesor de otro elemento) que es único (por S2), también el predecesor de a está en $|\mathfrak{A}|$ y lo mismo sucede con el predecesor del predecesor, etc. Todos estos elementos deben ser distintos, pues de otro modo se tendría un ciclo finito. Por lo tanto, a pertenece a una "Z-cadena":

$$\cdots * \to * \to a \to \mathbf{S}^{\mathfrak{A}}(a) \to \mathbf{S}^{\mathfrak{A}}(\mathbf{S}^{\mathfrak{A}}(a)) \to \cdots .$$

(Se les llama Z-cadenas porque están ordenadas como el conjunto de los enteros $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$.) Puede haber cualquier cantidad de Z-cadenas, pero deben ser ajenas dos a dos, ya que S2 prohíbe intersecciones entre ellas. También sucede que cualquier Z-cadena de un modelo es ajena a la parte estándar.

Este resultado puede plantearse de otra manera. Digamos que dos elementos a y b de $|\mathfrak{A}|$ son *equivalentes* si es posible pasar de uno de ellos al otro mediante la aplicación de la función $\mathbf{S}^{\mathfrak{A}}$ un número finito de veces. Es fácil ver que *se trata de* una

relación de equivalencia (está claro que es reflexiva y simétrica, y la transitividad se sigue del hecho de que $\mathbf{S}^{\mathfrak{A}}$ es inyectiva). La parte estándar de $|\mathfrak{A}|$ corresponde a la clase de equivalencia que contiene a $\mathbf{0}^{\mathfrak{A}}$. Para cualquier elemento a de $|\mathfrak{A}|$, la clase de equivalencia de a se genera a partir de $\{a\}$ aplicando $\mathbf{S}^{\mathfrak{A}}$ y su inversa. Esta clase de equivalencia corresponde a la **Z**-cadena antes descrita.

Inversamente, cualquier estructura $\mathfrak{B}$ (de este lenguaje) que contenga la parte estándar

$$\mathbf{0}^{\mathfrak{B}} \to \mathbf{S}^{\mathfrak{B}}(\mathbf{0}^{\mathfrak{B}}) \to \mathbf{S}^{\mathfrak{B}}(S^{\mathfrak{B}}(\mathbf{0}^{\mathfrak{B}})) \to \cdots$$

y una parte no estándar compuesta por Z-cadenas ajenas es modelo de A_S. (Puede verificarse que cada uno de los axiomas listados es verdadero en $\mathfrak{B}$). Con esto tenemos una caracterización completa de los modelos de A_S.

Si un modelo $\mathfrak{A}$ de A_S tiene sólo una cantidad numerable de Z-cadenas, entonces $|\mathfrak{A}|$ es numerable. En general, si el conjunto de Z-cadenas de $\mathfrak{A}$ tiene cardinalidad λ,[1] entonces la cantidad de elementos de $|\mathfrak{A}|$ es $\aleph_0 = \aleph_0 \cdot \lambda$. Y esto es, por aritmética cardinal (véase el capítulo cero), el máximo entre $\aleph_0$ y λ. Por lo tanto,

$$\text{card } |\mathfrak{A}| = \begin{cases} \aleph_0 & \text{si } \mathfrak{A} \text{ tiene una cantidad numerable de Z-cadenas.} \\ \lambda & \text{si } \mathfrak{A} \text{ tiene una cantidad no numerable } \lambda \text{ de Z-cadenas.} \end{cases}$$

Lema 31A Si $\mathfrak{A}$ y $\mathfrak{A}'$ son modelos de A_S con la misma cantidad de Z-cadenas, entonces son isomorfos.

Demostración Existe un único isomorfismo entre la parte estándar de $\mathfrak{A}$ y la parte estándar de $\mathfrak{A}'$. Además, por hipótesis, existe una correspondencia uno a uno entre el conjunto de Z-cadenas de $\mathfrak{A}$ y el conjunto de Z-cadenas de $\mathfrak{A}'$; es decir, cada Z-cadena de $\mathfrak{A}$ está asociada con una Z-cadena de $\mathfrak{A}'$, y viceversa. Queda claro que cualesquiera dos Z-cadenas son isomorfas. Al combinar todos estos isomorfismos particulares (usando el axioma de elección), tenemos un isomorfismo entre $\mathfrak{A}$ y $\mathfrak{A}'$. ⊣

[1] Es posible evitar cardinales no numerables; véase el ejercicio 3.

Por lo tanto, un modelo de A_S queda caracterizado, salvo isomorfismo, por la cantidad de Z-cadenas que contiene. Para el caso particular de $\mathfrak{N}_S$, el número de Z-cadenas es cero, pero es posible tener modelos con cualquier cantidad de Z-cadenas.

El lector debe darse cuenta de que no hay ningún enunciado del lenguaje que diga "No hay Z-cadenas". Lo que es más, no hay ningún conjunto Σ de enunciados tal que: un modelo $\mathfrak{A}$ de A_S satisfaga Σ sii $\mathfrak{A}$ no tiene Z-cadenas. Por el teorema LST existe una estructura $\mathfrak{A}$ no numerable tal que $\mathfrak{A} \equiv \mathfrak{A}_S$. Pero $\mathfrak{A}$ tiene un cantidad no numerable de Z-cadenas y $\mathfrak{N}_S$ no tiene ninguna.

Teorema 31B Sean $\mathfrak{A}$ y $\mathfrak{B}$ modelos no numerables de A_S con la misma cardinalidad. Entonces $\mathfrak{A}$ es isomorfo a $\mathfrak{B}$.

Demostración De la última discusión se desprende que $\mathfrak{A}$ y $\mathfrak{B}$ tienen, cada uno, una cantidad de Z-cadenas igual a sus cardinalidades (card$\mathfrak{A}$ y card $\mathfrak{B}$, respectivamente). Pero como card $\mathfrak{A}$ = card $\mathfrak{B}$, entonces $\mathfrak{A}$ y $\mathfrak{B}$ tienen la misma cantidad de Z-cadenas y, por lo tanto, son isomorfos. ⊣

Teorema 31C Cn A_S es una teoría completa.

Demostración Hay que aplicar la prueba de Loś-Vaught de la sección 6 del capítulo II. Por el teorema anterior tenemos que la teoría Cn A_S es *λ-categórica* para todo λ cardinal no numerable. Por otro lado, A_S no tiene modelos finitos. Por lo tanto, se cumplen las condiciones de la prueba de Loś-Vaught. ⊣

Corolario 31D Cn A_S = Th $\mathfrak{N}_S$.

Demostración Tenemos que Cn $A_S \subseteq$ Th $\mathfrak{N}_S$, donde la primera teoría es completa y la segunda satisfactible. ⊣

***Corolario 31E** Th $\mathfrak{N}_S$ es decidible.

Demostración Cualquier teoría completa y axiomatizable es decidible (por el corolario 25G). A_S es un conjunto decidible de axiomas para esta teoría. ⊣

Eliminación de cuantificadores

Una vez que sabemos que una teoría es decidible, resulta tentador tratar de encontrar un procedimiento concreto de decisión. Para el caso de Th $\mathfrak{N}_S$ daremos un procedimiento basado en "eliminación de cuantificadores".

Definición Una teoría T admite eliminación de cuantificadores sii para toda fórmula φ existe una fórmula ψ sin cuantificadores tal que

$$T \models (\varphi \leftrightarrow \psi).$$

En realidad, es suficiente con que se cumpla para cierto tipo de fórmulas φ:

Teorema 31F Supongamos que para toda fórmula φ de la forma

$$\exists x(\alpha_0 \wedge \cdots \wedge \alpha_n),$$

donde α_i ($i = 0, \ldots, n$) es una fórmula atómica o la negación de una fórmula atómica, existe una fórmula sin cuantificadores ψ tal que $T \models (\varphi \leftrightarrow \psi)$. Entonces T admite eliminación de cuantificadores.

Demostración Afirmamos que para toda fórmula de la forma $\exists x\theta$, donde θ carece de cuantificadores, podemos encontrar una fórmula equivalente sin cuantificadores. Comenzaremos escribiendo θ en forma normal disyuntiva (corolario 15C). La fórmula que se obtiene

$$\exists x[(\alpha_0 \wedge \cdots \wedge \alpha_m) \vee (\beta_0 \wedge \cdots \wedge \beta_n) \vee \cdots \vee (\xi_0 \wedge \cdots \wedge \xi_t)]$$

es lógicamente equivalente a

$$\exists x(\alpha_0 \wedge \cdots \wedge \alpha_m) \vee \exists x(\beta_0 \wedge \cdots \wedge \beta_n) \vee \cdots \vee \exists x(\xi_0 \wedge \cdots \wedge \xi_t).$$

Por hipótesis, cada subfórmula disyunta de esta fórmula disyuntiva puede sustituirse por una fórmula sin cuantificadores.

Dejamos al lector demostrar (ejercicio 2), a partir de lo expuesto en el párrafo anterior, que para toda fórmula es posible encontrar una fórmula equivalente sin cuantificadores. ⊣

Para el caso particular de la teoría Th $\mathfrak{A}$ de la estructura $\mathfrak{A}$, la definición puede replantearse de la siguiente manera: Th $\mathfrak{A}$ admite eliminación de cuantificadores sii para toda fórmula φ existe una fórmula ψ sin cuantificadores tal que φ y ψ son "equivalentes en $\mathfrak{A}$", es decir,

$$\models_{\mathfrak{A}} (\varphi \leftrightarrow \psi)[s]$$

para toda función s de las variables en $|\mathfrak{A}|$.

Teorema 31G Th $\mathfrak{N}_S$ admite eliminación de cuantificadores.

Demostración Por el teorema anterior, es suficiente considerar una fórmula del tipo

$$\exists x (\alpha_0 \wedge \cdots \wedge \alpha_q),$$

en la que cada α_i es una fórmula atómica o la negación de una fórmula atómica. Describiremos cómo sustituir esta fórmula por otra que no tenga cuantificadores. La equivalencia entre la nueva fórmula y la fórmula dada será una consecuencia de A_S; véase el ejercicio 3.

Los únicos términos del lenguaje $\mathfrak{N}_S$ son de la forma $\mathbf{S}^k u$, donde u es $\mathbf{0}$ o una variable. Las únicas fórmulas atómicas son ecuaciones. Podemos suponer que la variable x ocurre en todas las α_i. Puesto que si x no ocurre en α, entonces

$$\exists x (\alpha \wedge \beta) \models\!\!\dashv \alpha \wedge \exists x \beta.$$

Por lo tanto, toda α_i es de la forma

$$\mathbf{S}^m x = \mathbf{S}^n u$$

o la negación de esta ecuación, en la que u es $\mathbf{0}$ o una variable. Más aún, podemos suponer que u es distinta de x, pues $\mathbf{S}^m x = \mathbf{S}^n x$ puede sustituirse por $\mathbf{0} = \mathbf{0}$ si $m = n$, y por $\mathbf{0} \neq \mathbf{0}$ si $m \neq n$.

Caso 1: Toda α_i es la negación de una ecuación. Entonces la fórmula puede sustituirse por $\mathbf{0} = \mathbf{0}$ (¿Por qué?)

Caso 2: Existe al menos una α_i que no es la negación de una ecuación. Digamos que α_0 es

$$\mathbf{S}^m x = \mathbf{t},$$

donde t es un término que no contiene a x. Puesto que la solución de x debe ser no negativa, sustituimos α_0 por

$$t \neq \mathbf{0} \wedge \cdots \wedge t \neq \mathbf{S}^{m-1}\mathbf{0}$$

(o por $\mathbf{0} = \mathbf{0}$, si $m = 0$). Entonces en cada una de las α_j restantes sustituimos

$$\mathbf{S}^k x = u$$

primero por

$$\mathbf{S}^{k+m} x = \mathbf{S}^m u,$$

que se convierte en

$$\mathbf{S}^k t = \mathbf{S}^m u.$$

Tenemos entonces una fórmula en la que x ya no aparece, de modo que el cuantificador se puede eliminar. ⊣

Existen otras consecuencias secundarias muy interesantes del procedimiento de eliminación de cuantificadores. Por ejemplo, una demostración alternativa de la completud de Cn A_S. Supongamos que tenemos el enunciado σ. El procedimiento de eliminación de cuantificadores nos da un *enunciado* τ sin cuantificadores tal que (por el ejercicio 3) $A_S \models (\sigma \leftrightarrow \tau)$. Nosotros afirmamos que $A_S \models \tau$ o $A_S \models \neg\tau$, ya que τ se construye a partir de fórmulas atómicas y mediante los conectivos $\neg$ y $\rightarrow$. Todo enunciado atómico debe ser de la forma $\mathbf{S}^k\mathbf{0} = \mathbf{S}^l\mathbf{0}$; si $k = l$, entonces es deducible a partir de A_S; pero si $k \neq l$, entonces es refutable a partir de A_S (es decir, su negación es deducible). (Para demostrar esto, sólo se necesita $\{S1, S2\}$.) Ahora bien, como todo enunciado atómico es deducible o refutable, entonces lo mismo sucede con todo enunciado sin cuantificadores, lo que demuestra la afirmación. Por lo tanto, $A_S \models \sigma$ o $A_S \models \neg\sigma$.

Hay otra consecuencia importante relacionada con el problema de la definibilidad en $\mathfrak{N}_S$; véanse los ejercicios 4 y 5.

Para toda fórmula φ en la que sólo v_1 y v_2 ocurren libres, podemos encontrar una fórmula ψ sin cuantificadores (pero con las mismas variables libres) tal que

$$\mathrm{Th}\,\mathfrak{N}_S \models \forall v_1 \forall v_2 (\varphi \leftrightarrow \psi);$$

es decir,

$$\models_{\mathfrak{N}_S} \forall v_1 \forall v_2 (\varphi \leftrightarrow \psi).$$

Por lo tanto, la relación definida por φ también es definible a partir de una fórmula sin cuantificadores.

Ejercicios

1. Sea A_S^* el conjunto de enunciados conformado por S1, S2 y todos los enunciados de la forma

$$\varphi(0) \to \forall v_1(\varphi(v_1) \to \varphi(Sv_1)) \to \forall v_1\, \varphi(v_1),$$

   donde φ es una fórmula (del lenguaje $\mathfrak{N}_S$) que tiene a v_1 como única variable libre. Demuestre que $A_S \subseteq \mathrm{Cn}\,A_S^*$. Concluya que $\mathrm{Cn}\,A_S^* = \mathrm{Th}\,\mathfrak{N}_S$. (En este caso, $\varphi(t)$ es, por definición, $\varphi_t^{v_1}$. Al enunciado anterior se le conoce como el *axioma de inducción* para φ.)

2. Termine la demostración del teorema 31F. *Sugerencia:* Use inducción.

3. En la demostración de que $\mathrm{Th}\,\mathfrak{N}_S$ admite eliminación de cuantificadores se establece cómo encontrar, para toda fórmula φ, una fórmula ψ sin cuantificadores. Demuestre que

$$A_S \models (\varphi \leftrightarrow \psi)$$

   sin usar la completud de $\mathrm{Cn}A_S$. (Esto nos permite dar una demostración alternativa de la completud de $\mathrm{Cn}A_S$ que no involucre Z-cadenas o la prueba de Łoś-Vaught-Vaught.)

4. Demuestre que un subconjunto de $\mathbb{N}$ es definible en $\mathfrak{N}_S$ sii es finito o su complemento (en $\mathbb{N}$) es finito.

5. Demuestre que la relación de orden $\{\langle m,n\rangle \mid m < n$ en $\mathbb{N}\}$ no es definible en $\mathfrak{N}_S$. *Sugerencia*: Basta con demostrar que no hay una definición de orden sin cuantificadores. Una relación $R \subseteq \mathbb{N} \times \mathbb{N}$ es *lineal* si puede cubrirse mediante un número finito de líneas (es decir, subconjutos de $\mathbb{N}$ totalmente ordenados por R). Se dice que R es *colineal* si es el complemento de una relación lineal. Demuestre que toda relación definible en $\mathfrak{N}_S$ es lineal o colineal, y que la relación de orden no es ni lineal ni colineal.

6. Demuestre que $\mathrm{Th}\,\mathfrak{N}_S$ no es finitamente axiomatizable. *Sugerencia*: Demuestre que ningún subconjunto finito de A_S es suficiente para axiomatizar $\mathrm{Th}\,\mathfrak{N}_S$ y después use la sección 6 del capítulo 11.

2. *Otros reductos de la teoría de números*[2]

Primero agregamos el símbolo de orden < al lenguaje. La estructura propuesta para este caso es

$$\mathfrak{N}_L = (\mathbb{N}; 0, S, <).$$

Lo que queremos es demostrar que la teoría de esta estructura es decidible (como la de $\mathfrak{N}_S$) y admite eliminación de cuantificadores. Sin embargo, a diferencia de $\mathfrak{N}_S$, es finitamente axiomatizable y no es *λ-categórica* para ningún λ cardinal infinito.

El conjunto finito A_L de axiomas para la teoría $\mathrm{Th}\,\mathfrak{N}_L$ estará conformado por los seis enunciados que se presentan a continuación. En este caso, $x \leq y$ es una abreviatura de $(x < y \vee x = y)$ y $x \not\leq y$ de la negación.

$\forall y$	$(y \neq 0 \to \exists x\; y = Sx)$	(S3)
$\forall x \forall y$	$(x < Sy \leftrightarrow x \leq y)$	(L1)
$\forall x$	$x \not< 0$	(L2)
$\forall x \forall y$	$(x < y \vee x = y \vee y < x)$	(L3)
$\forall x \forall y$	$(x < y \to y \not< x)$	(L4)
$\forall x \forall y \forall z$	$(x < y \to y < z \to x < z)$	(L5)

[2] Esta sección puede omitirse sin que esto tenga un efecto desastroso.

Es fácil ver que estos seis axiomas son verdaderos en $\mathfrak{N}_L$. Por lo tanto, $\text{Cn}A_L \subseteq \text{Th}\,\mathfrak{N}_L$. Sin embargo, en el otro sentido, la inclusión no es obvia, así que es necesario demostrarla. Comenzaremos listando algunas de las consecuencias del conjunto de axiomas.

(1) $A_L \vdash \forall x\, x < \mathbf{S}x$.

Demostración Tómese x en lugar de y en L1. ⊣

(2) $A_L \vdash \forall x\, x \not< x$.

Demostración Tómese x en lugar de y en L4. ⊣

(3) $A_L \vdash \forall x\, \forall y\, (x \not< y \leftrightarrow y \leq x)$ (tricotomía).

Demostración Para "$\rightarrow$" use L3. Para "$\leftarrow$" use L4 y (2). ⊣

(4) $A_L \vdash \forall x \forall y (x < y \leftrightarrow \mathbf{S}x < \mathbf{S}y)$.

Demostración A partir de A_L se pueden deducir los siguientes bicondicionales:

$$\begin{aligned} x < y \leftrightarrow\ & y \not\leq x && \text{por (3);}\\ \leftrightarrow\ & y \not< \mathbf{S}x && \text{por L1;}\\ \leftrightarrow\ & \mathbf{S}x \leq y && \text{por (3);}\\ \leftrightarrow\ & \mathbf{S}x < \mathbf{S}y && \text{por L1.} \end{aligned}$$

⊣

(5) $A_L \vdash$ S1 y $A_L \vdash$ S2.

Demostración S1 se sigue de L2 y (1). S2 se deriva a partir de (4) usando L3 y (2). ⊣

(6) $A_L \vdash$ S4.n para $n = 1, 2, \ldots$

Demostración Se sigue de (1) y (2), usando L5. ⊣

Así pues, cualquier modelo $\mathfrak{A}$ de A_L también es modelo de A_S (si ignoramos $<^{\mathfrak{A}}$). Por lo tanto, debe consistir de una parte estándar sin más o una parte estándar junto con algunas Z-cadenas. Nótese, además, que está ordenado por $<^{\mathfrak{A}}$.

Teorema 32A La teoría $\text{Cn}\,A_L$ admite eliminación de cuantificadores.

Demostración Una vez más consideramos una fórmula de la forma

$$\exists x(\beta_0 \wedge \cdots \wedge \beta_p)$$

donde β_i $(i = 0, \ldots, p)$ es una fórmula atómica o la negación de una fórmula atómica. Los términos en este caso son, como en la sección 1 de este capítulo, de la forma $\mathbf{S}^k u$, donde u es $\mathbf{0}$ o una variable. Para las fórmulas atómicas hay dos posibilidades:

$$\mathbf{S}^k u = \mathbf{S}^l t \quad \text{o} \quad \mathbf{S}^k u < \mathbf{S}^l t.$$

1. Podemos eliminar el símbolo de negación. Gracias a L3 y L4 es posible sustituir $t_1 \not< t_2$ por $(t_2 < t_1 \vee t_1 = t_2)$ y sustituir $t_1 \neq t_2$ por $(t_1 < t_2 \vee t_2 < t_1)$. Ahora bien, haciendo las sustituciones correspondientes y notando que

$$\exists x(\varphi \vee \psi) \models\!\dashv \exists x\, \varphi \vee \exists x\, \psi,$$

podemos reagrupar fórmulas y reescribir la fórmula original como una disyunción de fórmulas del tipo:

$$\exists x(\alpha_0 \wedge \cdots \wedge \alpha_q),$$

donde α_i $(i = 0, \ldots, q)$ es ahora una fórmula atómica.

2. Podemos suponer que la variable libre x ocurre en toda α_i, pues si x no ocurre en α, entonces

$$\exists x(\alpha \wedge \beta) \models\!\dashv \alpha \wedge \exists x\, \beta.$$

Además podemos suponer que x ocurre en un solo lado de la igualdad o desigualdad α_i. Ya que $\mathbf{S}^k x = \mathbf{S}^l x$ puede reescribirse como se hizo en la sección 1 de este capítulo y $\mathbf{S}^k x < \mathbf{S}^l x$ puede sustituirse por $\mathbf{0} = \mathbf{0}$ si $k < l$, o $\mathbf{0} \neq \mathbf{0}$ si $l \leq k$ (lo que se justifica con L1 y L4).

Caso 1: Supongamos que al menos una α_i es una igualdad, entonces podemos proceder de la misma manera que para el caso 2 de la eliminación de cuantificadores del teorema 31G.

Caso 2: Todas las α_i son desigualdades. En este caso, la fórmula puede reescribirse de la siguiente manera:

$$\exists x \left(\bigwedge_i t_i < \mathbf{S}^{m_i} x \land \bigwedge_j \mathbf{S}^{n_j} x < u_j \right).$$

(Aquí, $\bigwedge_i$ denota la conjunción de fórmulas indexadas con i, de manera que $\gamma_0 \land \gamma_1 \land \cdots \land \gamma_k$ puede abreviarse como $\bigwedge_i \gamma_i$.) En la primera conjunción, $\bigwedge_i t_i < \mathbf{S}^{m_i} x$, tenemos las cotas inferiores de x, y en la segunda, $\bigwedge_j \mathbf{S}^{n_j} x < u_j$, las cotas superiores. Si la segunda conjunción es vacía (es decir, si no hay cotas superiores para x), entonces podemos sustituir la fórmula por $\mathbf{0} = \mathbf{0}$. (¿Por qué?) Si la primera conjunción es vacía (es decir, si no hay cotas inferiores para x), entonces podemos sustituir la fórmula por

$$\bigwedge_j \mathbf{S}^{n_j} \mathbf{0} < u_j,$$

que afirma que el $\mathbf{0}$ cumple con la desigualdad. En caso de que ninguna de las dos conjunciones sea vacía, reescribimos la fórmula sucesivamente hasta llegar a una fórmula sin cuantificadores:

$$\exists x \bigwedge_{i,j} (t_i < \mathbf{S}^{m_i} x \land \mathbf{S}^{n_j} x < u_j). \tag{1}$$

$$\exists x \bigwedge_{i,j} (\mathbf{S}^{n_j} t_i < \mathbf{S}^{m_i + n_j} x < \mathbf{S}^{m_i} u_j). \tag{2}$$

$$\left(\bigwedge_{i,j} \mathbf{S}^{n_j + 1} t_i < \mathbf{S}^{m_i} u_j \right) \land \bigwedge_j \mathbf{S}^{n_j} \mathbf{0} < u_j. \tag{3}$$

Esta última fórmula dice que "cualquier cota inferior más uno es menor que cualquier cota superior, y que el cero es menor que toda cota superior". Esto implica que la máxima cota inferior y la mínima cota superior no son consecutivas (es decir, que hay "espacio" entre ellas) y, por lo tanto, que existe solución para x. La segunda parte garantiza que la solución no puede ser negativa.

En cada caso pudimos encontrar una versión sin cuantificadores de la fórmula dada. ⊣

Corolario 32B (a) $\mathrm{Cn}A_L$ es completa.

(b) $\mathrm{Cn}A_L = \mathrm{Th}\,\mathfrak{N}_L$.

*(c) $\mathrm{Th}\,\mathfrak{N}_L$ es decidible.

Demostración (a) Se puede seguir el mismo argumento que se utilizó para la demostración del teorema 31G. (b) Se sigue del inciso (a), pues $\mathrm{Cn}\,A_L \subseteq \mathrm{Th}\,\mathfrak{N}_L$ y $\mathrm{Th}\,\mathfrak{N}_L$ es satisfactible. Para (c) se puede recurrir al hecho de que cualquier teoría completa axiomatizable es decidible. Sin embargo, la prueba que se usó para demostrar que $\mathrm{Cn}\,A_L$ admite eliminación de cuantificadores genera un procedimiento de decisión más eficiente. ⊣

Corolario 32C Un subconjunto de $\mathbb{N}$ es definible en $\mathfrak{N}_L$ sii es finito o tiene complemento finito.

Demostración Véase el ejercicio 4 de la sección anterior. ⊣

Cabe hacer notar que se pueden definir más relaciones binarias en $\mathfrak{N}_L$ que en $\mathfrak{N}_S$, pues la relación de orden $\{\langle m, n\rangle \mid m < n\}$ no se puede definir en $\mathfrak{N}_S$, por el ejercicio 5 de la sección anterior.

Corolario 32D La relación de suma

$$\{\langle m, n, p\rangle \mid m + n = p\}$$

no es definible en $\mathfrak{N}_L$.

Demostración Si se pudiera definir la suma en $\mathfrak{N}_L$, entonces también se podría definir en $\mathfrak{N}_L$ el conjunto de los números naturales pares. Pero dicho conjunto ni es finito ni tiene complemento finito. ⊣

Supongamos ahora que extendemos el lenguaje mediante el símbolo de suma $+$. En este caso, la estructura propuesta es

$$\mathfrak{N}_A = (\mathbb{N}; 0, S, <, +).$$

Probaremos que la teoría de esta estructura también es decidible; sin embargo, para evitar que las cosas se compliquen

demasiado, en este caso no daremos ninguna lista de axiomas para la teoría.

Los modelos no estándar de $\text{Th}\,\mathfrak{N}_A$ también deben ser modelos de $\text{Th}\,\mathfrak{N}_L$. Así que tienen una parte estándar y una parte compuesta por Z-cadenas. No obstante, en este caso, el orden entre las Z-cadenas ya no puede ser arbitrario. Sea $\mathfrak{A}$ un modelo no estándar de $\text{Th}\,\mathfrak{N}_A$. El orden $<^{\mathfrak{A}}$ induce un orden bien definido entre las Z-cadenas. (Véase el ejercicio 3.) Afirmamos que no hay una Z-cadena máxima en este nuevo orden, como tampoco una Z-cadena mínima; y además que, entre cualesquiera dos Z-cadenas, es posible encontrar otra Z-cadena. El argumento es, en términos generales, el siguiente: Si a pertenece a una Z-cadena (es decir, si es un elemento infinito de $\mathfrak{A}$), entonces $a +^{\mathfrak{A}} a$ pertenece a una Z-cadena más grande. Por otro lado, debe existir b tal que $b +^{\mathfrak{A}} b$ es a o el sucesor de a y, por lo tanto, b pertenece a una Z-cadena menor. Si a_1 y a_2 pertenecen a dos Z-cadenas distintas, entonces existe b tal que $b +^{\mathfrak{A}} b$ es $a_1 +^{\mathfrak{A}} a_2$ o su sucesor. En este caso, b pertenecería a una Z-cadena entre la Z-cadena de a_1 y la Z-cadena de a_2. (Con esto parece más o menos claro que estas afirmaciones son ciertas; aquellos que disfruten el manejo de números infinitos pueden completar los detalles.)

***Teorema 32E (Presburger, 1929)** La teoría de la estructura $\mathfrak{N}_A = (\mathbb{N}; 0, S, <, +)$ es decidible.

Esta demostración también está basada en un procedimiento de eliminación de cuantificadores, a pesar de que la teoría misma $\text{Th}\,\mathfrak{N}_A$ *no* admite eliminación de cuantificadores. Por ejemplo, la fórmula que define el conjunto de los números pares

$$\exists y\, v_1 = y + y$$

no tiene una fórmula equivalente sin cuantificadores. Este obstáculo desaparece si introducimos un nuevo símbolo $\equiv_2$ para la congruencia módulo 2. De manera similar agregamos los símbolos $\equiv_3, \equiv_4, \ldots$ La estructura propuesta para este lenguaje extendido será:

$$\mathfrak{N}^{\equiv} = (\mathbb{N}; 0, S, <, +, \equiv_2, \equiv_3, \ldots),$$

donde $\equiv_k$ es la relación binaria de congruencia módulo k. Resulta que la teoría de esta estructura sí permite eliminación de cuantificadores.

Esto no quiere decir, sin más, que la teoría de la estructura o de la estructura extendida sea decidible. Después de todo, *cualquier* estructura puede extenderse, agregando relaciones, hasta tener una estructura que permita eliminación de cuantificadores. Por lo tanto, para demostrar la decidibilidad, tenemos que probar dos cosas: (1) que dado cualquier enunciado σ, es posible dar, explícitamente, un enunciado equivalente σ' sin cuantificadores, y (2) que es posible decidir si σ' es verdadero.

Presentaremos ahora el procedimiento de eliminación de cuantificadores para Th $\mathfrak{N}^{\equiv}$. Dado un término t y un número natural n, sea nt el término de n sumandos $t + t + \cdots + t$. $0t$ es el $\mathbf{0}$. Así pues, todo término puede reescribirse como un término de la forma:

$$\mathbf{S}^{n_0}\mathbf{0} + n_1x_1 + \cdots + n_kx_k$$

con $k \geq 0$, $n_i \geq 0$ y los x_i como variables. Por ejemplo:

$$\mathbf{S}(x + \mathbf{S0}) + \mathbf{S}y$$

se puede sustituir por

$$\mathbf{S}^3\mathbf{0} + x + y.$$

Como siempre, empezamos con una fórmula del tipo $\exists y\,(\beta_1 \wedge \cdots \wedge \beta_n)$, donde $\beta_i\ (i = 0, \ldots, n)$ es una fórmula atómica o la negación de una fórmula atómica.

1. Eliminar la negación. Sustitúyase $\neg\,(t_1 = t_2)$ por $(t_1 < t_2 \vee t_2 < t_1)$. Sustitúyase $\neg\,(t_1 < t_2)$ por $(t_1 = t_2 \vee t_2 < t_1)$. Y sustitúyase $\neg\,(t_1 \equiv_m t_2)$ por:

$$t_1 \equiv_m t_2 = \mathbf{S}^1\mathbf{0} \vee \cdots \vee t_1 \equiv_m t_2 + \mathbf{S}^{m-1}\mathbf{0}.$$

Podemos, entonces, reescribir las negaciones y reagrupar fórmulas de modo que la fórmula original quede como una disyunción de fórmulas del tipo:

$$\exists y\,(\alpha_1 \wedge \cdots \wedge \alpha_m),$$

donde α_i $(i = 1, \ldots, n)$ es una fórmula atómica. Podemos suponer, como ya se ha hecho antes, que y ocurre en toda α_i, e incluso que α_i tiene alguna de las siguientes formas:

$$\begin{aligned} ny + t &= u, \\ ny + t &\equiv_m u, \\ ny + t &< u, \\ u &< ny + t, \end{aligned}$$

donde u y t son términos en los que no aparece y. De ahora en adelante nos tomaremos la libertad de escribir estas fórmulas usando un símbolo de resta:

$$\begin{aligned} ny &= u - t, \\ ny &\equiv_m u - t, \\ ny &< u - t, \\ u - t &< ny. \end{aligned}$$

Estas fórmulas simplemente son abreviaciones de las fórmulas anteriores, como se puede ver si se transponen los términos y se abandona el símbolo de resta.

Dicho todo lo anterior, está claro que nuestra fórmula dada puede ser, por ejemplo:

$$\exists y(w < 4y \wedge 2y < u \wedge 3y < v \wedge y \equiv_3 t),$$

donde t, u, v y w son términos en los que no aparece y.

2. Establecer un coeficiente común para y. Sea p el mínimo común múltiplo de los coeficientes de y. Cada fórmula atómica puede transformarse, "multiplicando" todos sus términos por un factor adecuado, en una fórmula en la que el coeficiente de y sea p. Queda claro que esto se puede hacer en el caso de las igualdades y las desigualdades. En el caso de las congruencias, también es necesario multiplicar el módulo por p, pues, en general,

$$a \equiv_m b \quad \text{sii} \quad ka \equiv_{km} kb.$$

En la fórmula del ejemplo anterior, p es 12, de modo que tendríamos:

$$\exists y(3w < 12y \wedge 12y < 6u \wedge 12y < 4v \wedge 12y \equiv_{36} 12t).$$

3. Eliminar el coeficiente de y. Sustitúyase py por x, y añádase la nueva fórmula atómica $x \equiv_p 0$. (Lo que nos dice esto es que en lugar de $\exists y \cdots 12y \cdots$ es posible tener "Existe un múltiplo x de 12 tal que $\cdots x \cdots$".) Entonces nuestro ejemplo puede sustituirse por

$$\exists x (3w < x \wedge x < 6u \wedge x < 4v \wedge x \equiv_{36} 12t \wedge x \equiv_{12} 0).$$

4. Caso especial. Si una de las fórmulas atómicas es una igualdad, $x + t = u$, entonces podemos reemplazar

$$\exists x \theta$$

por

$$\theta^x_{u-t} \wedge t \leq u.$$

Lo natural en este caso es sustituir x por "$u - t$", pero para evitar el uso del símbolo de resta transponemos términos. Por ejemplo:

$$(x \equiv_m v)^x_{u-t} \quad \text{corresponde a} \quad u \equiv_m v + t.$$

5. Caso general. Podemos suponer que la igualdad (=) no ocurre, entonces tenemos una fórmula de la forma

$$\begin{aligned} \exists x [& r_0 - s_0 < x \wedge \cdots \wedge r_{l-1} - s_{l-1} < x \\ & \wedge x < t_0 - u_0 \wedge \cdots \wedge x < t_{k-1} - u_{k-1} \\ & \wedge x \equiv_{m_0} v_0 - w_0 \wedge \cdots \wedge x \equiv_{m_{n-1}} v_{n-1} - w_{n-1}], \end{aligned}$$

donde r_i, s_i, t_i, u_i, v_i y w_i son términos en los que no aparece x. Esto puede abreviarse como

$$\exists x \left[\bigwedge_{j<l} r_j - s_j < x \wedge \bigwedge_{i<k} x < t_i - u_i \wedge \bigwedge_{i<n} x \equiv_{m_i} v_i - w_i \right].$$

Si no hay congruencias (es decir, si $n = 0$), entonces la fórmula afirma que hay *elementos* no negativos entre la máxima cota inferior y la mínima cota superior.

Así, pues, podemos sustituir la fórmula original por la siguiente fórmula sin cuantificadores:

$$\bigwedge_{i<k}\bigwedge_{j<l}(r_j - s_j) + \mathbf{S0} < t_i - u_i \wedge \bigwedge_{i<k} \mathbf{0} < t_i - u_i.$$

Sea M el mínimo común múltiplo de los módulos $m_0, \ldots, m_{n-1}$. Entonces $a + M \equiv_{mi} a$, de donde se ve que, a medida que a aumenta, el patrón de residuos de a módulo $m_0, \ldots, m_{n-1}$ tiene periodo M. Por lo tanto, para encontrar la solución de las congruencias, sólo necesitamos encontrar M enteros consecutivos.

Tenemos ahora una fórmula que asegura la existencia de un número natural que no es menor que determinadas cotas inferiores $L_1, \ldots, L_l$ y que satisface ciertas cotas superiores y ciertas congruencias. Si la solución existe, entonces debe ser alguno de los siguientes números:

$$\begin{array}{l} L_1, L_1 + 1, \ldots, L_1 + M - 1, \\ L_2, L_2 + 1, \ldots, L_2 + M - 1, \\ \ldots \\ L_l, L_l + 1, \ldots, L_l + M - 1, \\ 0, 1, \ldots, M - 1. \end{array}$$

(El último renglón es necesario para el caso en que todas las L_j sean negativas. Para evitar tener que tratar este renglón como un caso especial, incluimos el 0 como una nueva cota inferior. Es decir, sean $r_l = \mathbf{0}$ y $s_l = \mathbf{S0}$ tales que

$$r_l - s_l < x$$

es una fórmula $\mathbf{0} < x + \mathbf{S0}$ que afirma que x es no negativo. Con lo que tendríamos $l + 1$ cotas inferiores.)

Nuestra fórmula (que asegura la existencia de una solución para x) ahora puede sustituirse por una disyunción sin cuantificadores que afirma que alguno de los números de la matriz anterior es una solución no negativa:

$$\bigvee_{j\leq l}\bigvee_{1\leq q\leq M}\left[\bigwedge_{i\leq l} r_i - s_i < (r_j - s_j) + \mathbf{S}^q\mathbf{0}\right.$$
$$\wedge \bigwedge_{i<k}(r_j - s_j) + \mathbf{S}^q\mathbf{0} < t_i - u_i$$
$$\left.\wedge \bigwedge_{i<n}(r_j - s_j) + \mathbf{S}^q\mathbf{0} \equiv_{mi} v_i - w_i\right].$$

Retomando nuestro ejemplo, después de agregar la nueva cota inferior para x, tendríamos lo siguiente:

$$\exists x\,(3w < x \wedge \mathbf{0} < x + \mathbf{S0} \wedge x < 6u \wedge x < 4v$$
$$\wedge x \equiv_{36} 12t \wedge x \equiv_{12} \mathbf{0}).$$

La fórmula equivalente sin cuantificadores es una disyunción de 72 conjunciones, donde cada conjunción tiene seis componentes.

Hasta ahora sólo hemos probado la mitad del teorema. El procedimiento antes expuesto nos dice, dado un enunciado σ, cómo podemos encontrar un enunciado τ (en el lenguaje de $\mathfrak{N}^{\equiv}$) que no tenga cuantificadores y que sea verdadero (en la estructura propuesta para ese lenguaje) sii σ es verdadero. Sin embargo, falta decidir si τ es verdadero.

Pero esto es sencillo, pues basta considerar el caso de las fórmulas atómicas. Todo término sin variables puede escribirse en la forma $\mathbf{S}^n\mathbf{0}$. Entonces, por ejemplo,

$$\mathbf{S}^n\mathbf{0} \equiv_m \mathbf{S}^p\mathbf{0}$$

es verdadera sii $n \equiv_m p$. ⊣

Por lo tanto, tenemos un procedimiento de decisión para $\text{Th}\,\mathfrak{N}_A$. Sin embargo, en 1974, Michael Fischer y Michael Rabin demostraron que para fórmulas muy extensas no hay un procedimiento de decisión lo suficientemente rápido como para que se lleve a cabo en un "tiempo humano".

Se dice que un conjunto D de números naturales es *periódico* si existe un número positivo p tal que: n está en D sii $n + p$ está en D. D es *finalmente periódico* sii existen números positivos p

y M tales que, para todo n mayor que M, n está en D sii $n + p$ está en D.

Teorema 32F Un conjunto de números naturales es definible en $(\mathbb{N}; 0, S, <, +)$ sii es finalmente periódico.

Demostración El ejercicio 1 afirma que todo conjunto finalmente periódico es definible. Veamos la implicación contraria; supongamos que D es definible. Entonces D es definible en $\mathfrak{N}^{\equiv}$ mediante una fórmula sin cuantificadores (cuya única variable es v_1). Como la clase de los conjuntos finalmente periódicos es cerrada bajo unión, intersección y complemento, basta demostrar que toda fórmula atómica del lenguaje de $\mathfrak{N}^{\equiv}$ con v_1 como única variable define un conjunto finalmente periódico. Se tienen sólo cuatro posibilidades:

$$\begin{aligned} nv_1 + t &= u, \\ nv_1 + t &< u, \\ u &< nv_1 + t, \\ nv_1 + t &\equiv_m u, \end{aligned}$$

donde u y t son numerales. Las dos primeras fórmulas definen conjuntos finitos (que finalmente tienen periodo 1), la tercera define un conjunto que tiene complemento finito, y la última define un conjunto periódico con periodo m. ⊣

Corolario 32G La relación de multiplicación

$$\{\langle m, n, p\rangle \mid p = m \cdot n \text{ en } \mathbb{N}\}$$

no es definible en $(\mathbb{N}; 0, S, <, +)$.

Demostración Si hubiera una definición de la multiplicación, entonces podríamos usarla para definir el conjunto de los números cuadrados. Pero dicho conjunto no es finalmente periódico. ⊣

Ejercicios

1. Demuestre que cualquier conjunto finalmente periódico de números naturales es definible en la estructura $\mathfrak{N}_A$.

2. Demuestre que las siguientes relaciones son definibles en la estructura $(\mathbb{N}; +)$:

   (a) Orden $\{\langle m, n\rangle \mid m < n\}$.

   (b) Cero, $\{0\}$.

   (c) Sucesor $\{\langle m,n\rangle \mid n = S(m)\}$.

3. Sea $\mathfrak{A}$ un modelo de Th $\mathfrak{N}_L$ (o, lo que es lo mismo, un modelo de A_L). Dados a y b en $|\mathfrak{A}|$, definimos la siguiente relación de equivalencia:

   $a \sim b \iff \mathrm{S}^{\mathfrak{A}}$ puede aplicarse un número finito de veces a a para alcanzar a b, o viceversa.

   Sea $[a]$ la clase de equivalencia a la que pertenece a. Considérese el siguiente orden entre las clases de equivalencia:

   $$[a] \prec [b] \quad \text{sii} \quad a <^{\mathfrak{A}} b \quad \text{y} \quad a \not\sim b$$

   Demuestre que se trata de un orden bien definido para el conjunto de las clases de equivalencia.

4. Demuestre que la teoría de los números reales con su orden usual, Th $(\mathbb{R}; <)$ admite eliminación de cuantificadores. (Suponga que el lenguaje incluye la igualdad.)

3. *Una subteoría de la teoría de números*

Ahora retomaremos el lenguaje completo de la teoría de números que se describió en la sección cero de este capítulo. Los parámetros del lenguaje son $\forall$, **0**, S, $<$, $+$, $\cdot$ y **E**. La estructura propuesta para este lenguaje es

$$\mathfrak{N} = (\mathbb{N}; 0, S, <, +, \cdot, E).$$

En realidad, en $(\mathbb{N}; \cdot, E)$ es posible definir $\{0\}$, S, $<$ y $+$. (Véase el ejercicio 1.) En la sección 8 de este capítulo demostraremos que también en $(\mathbb{N}; +, \cdot)$ es posible definir E, así como

0, S y $<$. Así que es posible ahorrarse algunos parámetros. Sin embargo, nos daremos el lujo de trabajar con todos ellos (especialmente con $\mathbf{E}$) para simplificar algunas demostraciones.

Como veremos más adelante, Th $\mathfrak{N}$ es una teoría muy fuerte que no es ni decidible ni axiomatizable. El camino más adecuado para demostrar estos resultados (junto con otros relacionados) es concentrarse en una subteoría finitamente axiomatizable de Th $\mathfrak{N}$. Esta subteoría, como se señaló en la sección cero de este capítulo, deberá ser lo suficientemente fuerte como para poder representar (en un sentido que será precisado más adelante) resultados sobre conjuntos decidibles. La subteoría que hemos elegido es Cn A_E, donde A_E es el siguiente conjunto de enunciados. (Nótese que, como en la sección anterior, $x \leq y$ es la abreviación de $x < y \lor x = y$.)

Conjunto A_E de axiomas

$\forall x$	$\mathbf{S}x \neq \mathbf{0}$	(S1)
$\forall x \forall y$	$(\mathbf{S}x = \mathbf{S}y \rightarrow x = y)$	(S2)
$\forall x \forall y$	$(x < \mathbf{S}y \leftrightarrow x \leq y)$	(L1)
$\forall x$	$x \not< \mathbf{0}$	(L2)
$\forall x \forall y$	$(x < y \lor x = y \lor y < x)$	(L3)
$\forall x$	$x + \mathbf{0} = x$	(A1)
$\forall x \forall y$	$x + \mathbf{S}y = \mathbf{S}(x + y)$	(A2)
$\forall x$	$x \cdot \mathbf{0} = \mathbf{0}$	(M1)
$\forall x \forall y$	$x \cdot \mathbf{S}y = x \cdot y + x$	(M2)
$\forall x$	$x\mathbf{E}\mathbf{0} = \mathbf{S}\mathbf{0}$	(E1)
$\forall x \forall y$	$x\mathbf{E}\mathbf{S}y = x\mathbf{E}y \cdot x$	(E2)

Como $\mathfrak{N}$ es un modelo de A_E, entonces Cn $A_E \subseteq$ Th $\mathfrak{N}$. Sin embargo, en este caso no se tiene la igualdad (como probaremos más adelante, en la sección 5). De hecho, se puede probar que $A_E \nvdash$ S3, donde S3 es el enunciado $\forall y\ (y \neq \mathbf{0} \rightarrow \exists x\ y = \mathbf{S}x)$.

Los primeros cinco enunciados son *algunos* de los axiomas relacionados con $\mathbf{S}$ y $<$ que se utilizaron en las secciones anteriores, aunque no todos. Los seis restantes son las ecuaciones

"recursivas" que definen la suma, la multiplicación y la exponenciación.

Lo primero que haremos es demostrar que algunos enunciados sencillos de Th $\mathfrak{N}$ se pueden deducir a partir de A_E.

Lema 33A (a) $A_E \vdash \forall x\, x \not< \mathbf{0}$.

(b) Dado cualquier número natural k,

$$A_E \vdash \forall x (x < \mathbf{S}^{k+1}\mathbf{0} \leftrightarrow x = \mathbf{S}^0\mathbf{0} \vee \cdots \vee x = \mathbf{S}^k\mathbf{0}).$$

Nótese que (a) puede verse como el caso $k = -1$ del inciso (b), en el que la disyunción vacía es $\perp$. Este lema nos dice que A_E "sabe", por ejemplo, que los números menores que 7 son exactamente 0, 1, 2, 3, 4, 5 y 6. De modo que en cualquier modelo de A_E, los elementos estándar —denotados por los numerales $S^k\mathbf{0}$— están ordenados de la manera usual, y (por L3) todos los elementos infinitos, si es que los hay, son mayores que cualquier elemento estándar.

Demostración El inciso (a) es L2. Para el inciso (b) utilizaremos inducción (en español) sobre k. Como consecuencia de L1 tenemos:

$$x < \mathbf{S0} \leftrightarrow x < \mathbf{0} \vee x = \mathbf{0},$$

que junto con L2 nos da

$$x < \mathbf{S0} \leftrightarrow x = \mathbf{0}.$$

Éste es el caso $k = 0$ del inciso (b). Para el paso inductivo aplicamos, una vez más, L1:

$$x < \mathbf{S}^{k+1}\mathbf{0} \leftrightarrow x < \mathbf{S}^k\mathbf{0} \vee x = \mathbf{S}^k\mathbf{0}.$$

Usando la hipótesis de inducción, $x < \mathbf{S}^k\mathbf{0}$ puede sustituirse por

$$x = \mathbf{S}^0\mathbf{0} \vee \cdots \vee x = \mathbf{S}^{k-1}\mathbf{0},$$

con lo que finalmente tendríamos (b). ⊣

Lemas 33B Para todo término t sin variables, existe un único número natural n tal que

$$A_E \vdash t = \mathbf{S}^n\mathbf{0}.$$

Demostración La unicidad es inmediata. (¿Por qué? Porque A_E no es muy fuerte, pero al menos sabe, por S1, que $7 \neq 0$ y que $87 \neq 80$ recurriendo a S2 ochenta veces.) Para demostrar la existencia utilizaremos inducción sobre t. Si t es $\mathbf{0}$, entonces tomamos $n = 0$. Si t es $\mathbf{S}u$, entonces, por hipótesis de inducción $A_E \vdash u = \mathbf{S}^m\mathbf{0}$ para alguna m. Por lo tanto, $A_E \vdash t = \mathbf{S}^{m+1}\mathbf{0}$.

Supongamos ahora que t es $u_1 + u_2$. Por hipótesis de inducción $A_E \vdash t = \mathbf{S}^m\mathbf{0} + \mathbf{S}^n\mathbf{0}$ para algunas m y n. Aplicamos ahora A2 n veces y A1 una vez para obtener $A_E \vdash t = \mathbf{S}^{m+n}\mathbf{0}$. Los argumentos para la multiplicación y la exponenciación son similares. ⊣

Como caso particular de este lema tenemos que "$2 + 2 = 4$" (es decir, $\mathbf{S}^2\mathbf{0} + \mathbf{S}^2\mathbf{0} = \mathbf{S}^4\mathbf{0}$) es consecuencia de A_E. Vemos entonces que A_E es al menos lo suficientemente inteligente como para determinar los términos sin variables. De hecho, la demostración dice más, pues nos da las instrucciones exactas para que, dado un término t sin variables, podamos encontrar el único número n tal que $A_E \vdash t = \mathbf{S}^n\mathbf{0}$.

Teorema 33C Para todo enunciado τ sin cuantificadores verdadero en $\mathfrak{N}$, $A_E \vdash \tau$.

Demostración Ejercicio 2. Comience con los enunciados atómicos; éstos serán de la forma $t_1 = t_2$ o $t_1 < t_2$, donde t_1 y t_2 son términos sin variables. Demuestre que A_E prueba τ si τ es verdadero en $\mathfrak{N}$ y que refuta τ (es decir, que prueba $\neg\tau$) si τ es falso en $\mathfrak{N}$. ⊣

Más adelante daremos una versión más amplia del teorema 33C en la que se permite que τ tenga "cuantificadores acotados"; véase el teorema 33I.

Simplificar la notación de la sustitución (como ya se hizo en la sección 7 del capítulo II) será de gran utilidad en las siguientes páginas:

$$\varphi(t) = \varphi^{v_1}_t$$
$$\varphi(t_1, t_2) = (\varphi^{v_1}_{t_1})^{v_2}_{t_2},$$

y así sucesivamente. De modo que $\varphi = \varphi(v_1) = \varphi(v_1, v_2)$. Por lo general, el término sustituido será un numeral, por ejemplo:

$$\varphi(\mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0}) = (\varphi^{\boldsymbol{v}_1}_{\mathbf{S}^a\mathbf{0}})^{\boldsymbol{v}_2}_{\mathbf{S}^b\mathbf{0}}.$$

Sin embargo, en algunas casos también sustituiremos otro tipo de términos; por ejemplo, $\varphi(x) = \varphi^{\boldsymbol{v}_1}_x$, donde x es una variable. No obstante, si x no es sustituible por $\boldsymbol{v}_1$ en φ, entonces tenemos que tomar $\varphi(x) = \psi^{\boldsymbol{v}_1}_x$, donde ψ es una variante alfabética adecuada de φ.

En la demostración del siguiente corolario (así como en otras partes de este capítulo) usaremos la consecuencia del lema de sustitución de la sección 5 del capítulo II: para toda fórmula φ en la que al menos $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ ocurren libres y para todo número natural $a_1, \ldots, a_n$,

$$\models_{\mathfrak{N}} \varphi[[a_1, \ldots, a_n]] \Leftrightarrow \models_{\mathfrak{N}} \varphi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_n}\mathbf{0}).$$

Una fórmula existencial ($\exists_1$) es una fórmula de la forma $\exists x_1 \cdots \exists x_k\, \theta$, donde θ carece de cuantificadores. El siguiente resultado es una versión más fuerte del teorema 33C:

Corolario 33D Si τ es un enunciado existencial verdadero en $\mathfrak{N}$, entonces $A_E \vdash \tau$.

Demostración Si $\exists \boldsymbol{v}_1 \exists \boldsymbol{v}_2\, \theta$ es verdadero en $\mathfrak{N}$, entonces $\theta(\mathbf{S}^m\mathbf{0}, \mathbf{S}^n\mathbf{0})$ es verdadero en $\mathfrak{N}$ para algunos números naturales m y n. Este último es un enunciado verdadero sin cuantificadores, así que es deducible a partir de A_E, pero además implica lógicamente $\exists \boldsymbol{v}_1 \exists \boldsymbol{v}_2\, \theta$. ⊣

Por otro lado, sabemos que hay enunciados universales ($\forall_1$) verdaderos (es decir, de la forma $\forall x_1 \cdots \forall x_k \theta$, con θ sin cuantificadores) que *no* están en $\operatorname{Cn} A_E$.

Relaciones representables

Sea R una relación m-aria sobre $\mathbb{N}$; es decir, $R \subseteq \mathbb{N}^m$. Sabemos que una fórmula ρ (en la que $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ ocurren libres) define R en $\mathfrak{N}$ sii para toda $a_1, \ldots, a_m$ en $\mathbb{N}$,

$$\begin{aligned}\langle a_1, \ldots, a_m\rangle \in R &\Leftrightarrow \models_{\mathfrak{N}} \rho[[a_1, \ldots, a_m]]\\ &\Leftrightarrow \models_{\mathfrak{N}} \rho(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}).\end{aligned}$$

(La última condición es equivalente a la anterior por el lema de sustitución.) Podemos reescribir esto último mediante dos implicaciones:

$$\langle a_1, \ldots, a_m \rangle \in R \Rightarrow \models_{\mathfrak{N}} \rho(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}),$$
$$\langle a_1, \ldots, a_m \rangle \notin R \Rightarrow \models_{\mathfrak{N}} \neg \rho(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}).$$

Diremos que ρ también representa R en la teoría $\mathrm{Cn}A_E$ si, en estas dos últimas implicaciones, la noción de verdad en $\mathfrak{N}$ puede sustituirse por la noción más fuerte de deducción a partir de A_E.

De manera más general, sea T cualquier teoría en un lenguaje con $\mathbf{0}$ y $\mathbf{S}$. Entonces ρ *representa* R en T sii para toda $a_1, \ldots, a_m$ en $\mathbb{N}$:

$$\langle a_1, \ldots, a_m \rangle \in R \Rightarrow \rho(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}) \in T,$$
$$\langle a_1, \ldots, a_m \rangle \notin R \Rightarrow (\neg \rho(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})) \in T.$$

Por ejemplo, ρ representa R en la teoría $\mathrm{Th}\,\mathfrak{N}$ sii ρ define R en $\mathfrak{N}$. Pero ρ representa R en $\mathrm{Cn}\,A_E$ sii para toda $a_1, \ldots, a_m$ en $\mathfrak{N}$:

$$\langle a_1, \ldots, a_m \rangle \in R \Rightarrow A_E \vdash \rho(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}),$$
$$\langle a_1, \ldots, a_m \rangle \notin R \Rightarrow A_E \vdash \neg \rho(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}).$$

La relación de igualdad en $\mathbb{N}$, por ejemplo, está representada en $\mathrm{Cn}A_E$ por la fórmula $v_1 = v_2$, ya que

$$m = n \Rightarrow \vdash \mathbf{S}^m\mathbf{0} = \mathbf{S}^n\mathbf{0}$$
$$m \neq n \Rightarrow \{S1, S2\} \vdash \neg \mathbf{S}^m\mathbf{0} = \mathbf{S}^n\mathbf{0}.$$

Una relación es *representable* en T sii existe alguna fórmula que la representa en T.

Comparemos el concepto de representabilidad con el de definibilidad. En ambos casos estamos, de alguna manera, describiendo relaciones entre números naturales a través de fórmulas. En el caso de la definibilidad, nos preguntamos acerca de la *verdad* de los enunciados en la interpretación, mientras que, en el caso de la representabilidad en $\mathrm{Cn}A_E$, nos preguntamos más bien si los enunciados son *deducibles* a partir de los axiomas.

Decimos que una fórmula φ, con $v_1, \ldots, v_m$ como únicas variables libres, está *numeralmente determinada* por A_E sii para toda m-ada $a_1, \ldots, a_m$ de números naturales, o bien

$$A_E \vdash \varphi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$$

o bien

$$A_E \vdash \neg \varphi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$$

Teorema 33E Una fórmula ρ representa una relación R en $\text{Cn}A_E$ sii

(1) ρ está numeralmente determinada por A_E, y

(2) ρ define R en $\mathfrak{N}$.

Demostración Usaremos el hecho de que $\mathfrak{N}$ es modelo de A_E. Si ρ representa R en $\text{Cn}A_E$, entonces está claro que tenemos (1). El inciso (2) se desprende de que "$A_E \vdash$" implica que "$\models_{\mathfrak{N}}$". A la inversa, si (1) y (2) son ciertos, entonces tenemos que

$\langle a_1, \ldots, a_m \rangle \in R$	$\Rightarrow\ \models_{\mathfrak{N}} \rho(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$	por (2)
	$\Rightarrow A_E \nvdash \neg \rho(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$	pues $\mathfrak{N}$ es un modelo de A_E
	$\Rightarrow A_E \vdash \rho(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$	por (1).

Se puede obtener el resultado análogo para el complemento de R y $\neg \rho$. ⊣

La tesis de Church

Ahora nos concentraremos en la relación que hay entre los conceptos de representabilidad y decidibilidad.

***Teorema 33F** Supongamos que R es una relación representable en una teoría consistente y axiomatizable, entonces R es decidible.

Demostración Supongamos que ρ representa R en una teoría consistente y axiomatizable T. Recuérdese que T es efectivamente numerable (corolario 25F). El procedimiento de decisión es el siguiente:

Dados $a_1, \ldots, a_m$, enumeremos los elementos de T. Si $\rho(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$ se encuentra en algún lugar de la lista, entonces terminamos y $\langle a_1, \ldots, a_m \rangle \in R$. Si, en cambio, en la lista se encuentra $\neg \rho(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$, entonces terminamos y $\langle a_1, \ldots, a_m \rangle \notin R$.

Gracias a la representabilidad sabemos que alguno de estos dos enunciados debe aparecer en algún momento en la lista, por lo que tenemos garantizado que el procedimiento termina. Como T es consistente, entonces el resultado que arroja este procedimiento es correcto. ⊣

***Corolario 33G** Toda relación representable en una teoría consistente y finitamente axiomatizable es decidible.

Parecería natural preguntarse qué sucede con el inverso de este corolario. Lo que diremos es que no podemos pretender *demostrar* el inverso de este corolario basándonos en la noción informal de decidibilidad que hemos manejado hasta ahora, pues esta aproximación sólo nos sirve para dar una cota inferior de la clase de las relaciones decidibles (es decir, para demostrar que ciertas relaciones *son* decidibles), pero no es adecuada para dar cotas superiores (es decir, para mostrar *indecidibilidad*).

No obstante, es posible ofrecer argumentos a favor del inverso de este corolario, pero será más fácil hacerlo al final de la sección 4 de este capítulo. La idea intuitiva es que en un número finito de axiomas podríamos capturar las instrucciones (finitas) del procedimiento de decisión.

La afirmación de que este corolario junto con su inverso son ciertos es lo que comúnmente se conoce como la *tesis de Church*. En realidad, esta afirmación no es un enunciado matemático susceptible de prueba o refutación; más bien se trata de una postura matemática que propone que la manera más adecuada de formalizar la noción informal de decidibilidad es mediante la noción de representabilidad en teorías consistentes y finitamente axiomatizables.

Definición Una relación R sobre números naturales es *recursiva* sii es representable en alguna teoría consistente finitamente axiomatizable (en un lenguaje con **0** y **S**).

La tesis de Church se puede expresar de manera más sucinta: una relación es decidible sii es recursiva. Dicho con mayor precisión: el concepto de recursión es la versión correcta y precisa del concepto informal de decidibilidad. Esta situación es

análoga al caso de las funciones continuas dentro del cálculo. Intuitivamente decimos que una función es continua (definida en un intervalo) si su gráfica puede dibujarse sin levantar el lápiz del papel; sin embargo, para demostrar teoremas es necesario dar una versión formal de continuidad, así que solemos trabajar con la definición ε-δ de continuidad. Cabe preguntarse, empero, si la definición precisa ε-δ de continuidad corresponde verdaderamente a la idea intuitiva de continuidad. En realidad, la clase de funciones ε-δ continuas es bastante más amplia e incluye funciones que no son diferenciables en ninguna parte, cuyas gráficas no pueden trazarse sin levantar el lápiz. Pero, corresponda o no a la idea intuitiva, la clase de las funciones ε-δ continuas ha resultado ser muy natural e importante en el análisis matemático.

El caso de la recursividad es bastante similar, así que deberíamos preguntarnos si la noción precisa de recursividad es la formalización adecuada de la noción informal de decidibilidad. Un vez más, la clase bien definida de las relaciones recursivas parece ser muy amplia, pues incluye relaciones para las que cualquier procedimiento de decisión requeriría tantos cálculos y tanta memoria que sería absurdo intentar realizarlo. Podríamos decir, entonces, que recursividad corresponde a decidibilidad en un mundo ideal en el que la cantidad de cálculos y la memoria que se ocupan no son un problema. Como sea, también en este caso la clase de las relaciones recursivas ha resultado ser una clase muy natural e importante dentro de la lógica matemática.

A continuación ofreceremos algunos argumentos empíricos para mostrar la amplitud de la clase de las relaciones recursivas:

1. Hasta ahora, toda relación que los matemáticos han intuido que es decidible ha resultado ser recursiva.

2. Varias personas han intentado dar definiciones precisas de máquinas computacionales ideales para realizar cálculos. Las más conocidas son las "máquinas de Turing", presentadas por Alan Turing en 1936. (Una variante de la idea de Turing nos lleva a las máquinas registradoras que se describen en la sección 6 de este capítulo.) La idea ha sido concebir algo que

pueda realizar cualquier procedimiento efectivo de decisión. En todos los casos, la clase de las relaciones que tienen un proceso de decisión ejecutable con alguna de estas máquinas corresponde a la clase de las relaciones recursivas. (La importancia del análisis de Turing sobre la calculabilidad efectiva hace que a la tesis de Church muchas veces se la denomine la *tesis de Church-Turing.*)

El hecho de que se hayan encontrado tantas definiciones distintas (aunque equivalentes) de la clase de las relaciones recursivas es un indicador de lo natural e importante que resulta dicho concepto.

En este libro seguiremos excluyendo la noción intuitiva de decidibilidad en los teoremas sin asterisco; pero en el resto de la exposición aceptaremos la tesis de Church. Por ejemplo, diremos que un conjunto es indecidible cuando tengamos un teorema que afirme que no es recursivo.

Es evidente que toda relación representable en Cn A_E es recursiva. Más adelante probaremos que el inverso también se cumple: si una relación es representable en cualquier teoría consistente y finitamente axiomatizable, entonces es representable en la teoría que hemos elegido estudiar. (Por supuesto, este resultado determinó en parte nuestra elección.)

El uso de la palabra "recursiva" es, en este caso, resultado de un accidente histórico, por no decir que de un error histórico. Recientemente, varios matemáticos han dicho que la palabra "calculable" refleja mejor las ideas involucradas; no obstante, nosotros queremos reservar la palabra "calculable" para otro concepto informal que definiremos a continuación. Así como para el caso de las relaciones tenemos el concepto informal de decidibilidad, para el caso de las funciones tenemos el concepto de calculabilidad. (Como una forma de simplificar la notación escribiremos $\vec{a}$ en lugar de $a_1, \ldots, a_n$.)

*Definición Una función $f: \mathbb{N}^n \to \mathbb{N}$ es *calculable* sii existe un procedimiento efectivo tal que, dada cualquier n-ada $\vec{a}$ de números naturales, nos da $f(\vec{a})$.

Por ejemplo, la suma y la multiplicación son calculables. Algunos procedimientos efectivos para estas funciones, usando

base 10, se enseñan en las escuelas primarias. (Si quisiéramos ser muy rigurosos en nuestra definición, en lugar de hablar de números naturales dados, tendríamos que hablar de *numerales*, pues son los numerales –sucesiones de símbolos como la terna 317 o la terna XCI– los que pueden expresarse mediante el lenguaje; sin embargo, haremos caso omiso de este detalle.) Por otro lado, dentro del conjunto no numerable de funciones de $\mathbb{N}^n$ en $\mathbb{N}$, sólo hay una cantidad numerable de funciones calculables, pues sólo hay una cantidad numerable de procedimientos efectivos.

Como en el caso de las relaciones decidibles, quisiéramos dar la versión formal del concepto de calculabilidad. La clave para encontrar la versión correcta nos la da el siguiente teorema. Recuérdese que cualquier función $f : \mathbb{N}^n \to \mathbb{N}$ es también una relación $(n + 1)$-aria sobre $\mathbb{N}$:

$$\langle a_1, \ldots, a_n, b\rangle \in f \Longleftrightarrow f(a_1, \ldots, a_n) = b.$$

Durante algún tiempo fue común distinguir entre la función y la relación (que se conocía como la *gráfica* de la función). Hoy en día, dentro de la teoría de conjuntos, se considera lo mismo una función que su gráfica, pero en realidad seguimos teniendo dos formas distintas de pensar una función.

***Teorema 33H** Las siguientes tres propiedades de una función $f : \mathbb{N}^n \to \mathbb{N}$ son equivalentes:

(a) f es calculable

(b) Vista como relación, f es decidible.

(c) Vista como relación, f es efectivamente numerable.

Demostración (a) $\Rightarrow$ (b): Supongamos que f es calculable; entonces describiremos el procedimiento de decisión. Dada $\langle a_1, \ldots, a_n, b\rangle$, primero calculamos $f(a_1, \ldots, a_n)$; después vemos si el resultado es igual a b. Si lo es, entonces decimos "sí"; si no lo es, decimos "no".

(b) $\Rightarrow$ (c): Cualquier relación decidible es efectivamente numerable, ya que es posible listar los elementos del conjunto de todas las $(n + 1)$-adas de números y

hacer una sublista de las que pasan la prueba de pertenencia a la relación.

(c) $\Rightarrow$ (a): Supongamos que tenemos una enumeración efectiva de (la gráfica de) f. Para calcular $f(a_1, \ldots, a_n)$ examinamos la lista de las $(n + 1)$-adas de f hasta que encontremos la que comienza con $a_1, \ldots, a_n$. La última componente de dicha $(n + 1)$-ada será el valor buscado de la función. ⊣

Por lo tanto, usando la tesis de Church, podemos decir que f es calculable sii f (vista como relación) es recursiva. La clase de las funciones recursivas, además de ser importante por su conexión con los teoremas de incompletud de la lógica matemática, es una clase muy interesante. Constituye una cota superior de la clase de las funciones que realmente pueden ser calculadas mediante programas para computadoras digitales. Las funciones recursivas son aquellas que son calculables mediante una computadora digital, siempre y cuando hagamos caso omiso de las limitaciones prácticas de tiempo y memoria que requieren los cálculos.

Ahora podemos decir cuáles son nuestros planes para las siguientes dos secciones. Nuestra meta principal es obtener los teoremas de la sección 5 de este capítulo; sin embargo, antes de demostrar los teoremas, es necesario obtener algunos resultados que servirán de base para las demostraciones: necesitamos verificar que un conjunto de relaciones (intuitivamente decidibles) y de funciones (intuitivamente calculables) son representables en Cn A_E y, por lo tanto, son recursivas. Sobre la marcha demostraremos (teorema 34A) que la recursividad es equivalente a la representabilidad en Cn A_E. En lo que queda de esta sección presentaremos algunos resultados generales sobre representabilidad. Además demostraremos, por ejemplo, que ciertas funciones que codifican sucesiones finitas de números mediante números son representables. En la sección 4 de este capítulo aplicaremos estos resultados a relaciones y funciones vinculadas a las características sintácticas del lenguaje formal.

El autor es consciente de que muchos lectores estarán más interesados en los teoremas de la sección 5 de este capítulo que en el trabajo preparatorio. Si el lector está dispuesto a aceptar

que las relaciones intuitivamente decidibles son representables en $\text{Cn}A_E$ y que las funciones intuitivamente calculables son funcionalmente representables en $\text{Cn}A_E$ (noción que pronto definiremos), entonces no será necesaria prácticamente ninguna, sino es que ninguna de las pruebas de los preparativos. No obstante, es deseable que se revisen las definiciones y los enunciados de los resultados previos.

Fórmulas numeralmente determinadas

El teorema 33E nos dice que podemos demostrar que una relación es representable en $\text{Cn}\,A_E$ si encontramos una fórmula que la defina en $\mathfrak{N}$ y que esté numeralmente determinada por A_E. El siguiente teorema se refiere a la determinación numeral.

Teorema 33I (a) Toda fórmula atómica está numeralmente determinada por A_E.

(b) Si φ y ψ están numeralmente determinadas por A_E, entonces $\neg\varphi$ y $\varphi \rightarrow \psi$ también lo están.

(c) Si φ está numeralmente determinada por A_E, entonces también lo están las siguientes fórmulas (que se obtienen a partir de φ mediante la "cuantificación acotada"):

$$\forall x(x < y \rightarrow \varphi),$$
$$\exists x(x < y \wedge \varphi).$$

Demostración El inciso (a) se sigue del teorema 33C y el inciso (b) es fácil de probar; así que sólo queda demostrar el inciso (c). Consideremos una fórmula del tipo

$$\exists x(x < y \wedge \varphi(x, y, z))$$

donde y y z son variables libres. Consideremos dos números naturales a y b; tenemos que demostrar que o bien

$$A_E \vdash \exists x(x < \mathbf{S}^a\mathbf{0} \wedge \varphi(x, \mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0}))$$

o bien

$$A_E \vdash \neg\exists x(x < \mathbf{S}^a\mathbf{0} \wedge \varphi(x, \mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0})).$$

Caso 1: Para alguna c menor que a,

$$A_E \vdash \varphi(\mathbf{S}^c\mathbf{0}, \mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0}). \quad (1)$$

(Este caso ocurre sii $\exists x(x < \mathbf{S}^a\mathbf{0} \wedge \varphi(x, \mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0}))$ es verdadero en $\mathfrak{N}$.) También tenemos

$$A_E \vdash \mathbf{S}^c\mathbf{0} < \mathbf{S}^a\mathbf{0}. \quad (2)$$

Los enunciados (1) y (2) implican lógicamente el siguiente enunciado:

$$\exists x(x < \mathbf{S}^a\mathbf{0} \wedge \varphi(x, \mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0})).$$

Caso 2: Para toda c menor que a,

$$A_E \vdash \neg\varphi(\mathbf{S}^c\mathbf{0}, \mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0}). \quad (3)$$

(Este caso ocurre sii $\forall x(x < \mathbf{S}^a\mathbf{0} \rightarrow \neg\varphi(x, \mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0}))$ es verdadero en $\mathfrak{N}$.) Por el lema 33A sabemos que

$$A_E \vdash \forall x(x < \mathbf{S}^a\mathbf{0} \rightarrow x = \mathbf{S}^0\mathbf{0} \vee \cdots \vee x = \mathbf{S}^{a-1}\mathbf{0}). \quad (4)$$

El enunciado (4) junto con los enunciados incluidos en (3) (para $c = 0, \ldots, a-1$) implican lógicamente que

$$\forall x(x < \mathbf{S}^a\mathbf{0} \rightarrow \neg\varphi(x, \mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0})).$$

Lo que es equivalente a

$$\neg\exists x(x < \mathbf{S}^a\mathbf{0} \wedge \varphi(x, \mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0})).$$

Esto demuestra que $\exists x(x < y \wedge \varphi(x,y,z))$ está numeralmente determinada por A_E. Si aplicamos este resultado a $\neg\varphi$, tenemos que la fórmula dual $\forall x(x < y \rightarrow \varphi(x,y,z))$ también está numeralmente determinada por A_E. ⊣

El argumento para el caso 2 es válido porque el cuantificador en x está acotado por $\mathbf{S}^a\mathbf{0}$. Más adelante veremos que es posible que

$$\neg\psi(\mathbf{S}^0\mathbf{0}), \neg\psi(\mathbf{S}^1\mathbf{0}), \ldots$$

sean todas consecuencias de A_E y que, sin embargo, no se tenga

$$\forall x \neg \psi(x)$$

como consecuencia de A_E.

El teorema anterior resulta ser una herramienta muy útil para demostrar que diversas relaciones son representables en $\mathrm{Cn}\, A_E$. Por ejemplo, el conjunto de los números primos está representado por

$$\mathbf{S}^1\mathbf{0} < v_1 \wedge \forall x (x < v_1 \to \forall y (y < v_1 \to x \cdot y \neq v_1)).$$

Esta fórmula que define los números primos en $\mathfrak{N}$, por el teorema anterior, está numeralmente determinada por A_E. Por lo tanto, esta fórmula representa a los números primos en $\mathrm{Cn}\, A_E$.

Funciones representables

Por lo general resulta más conveniente trabajar con funciones que con relaciones. Así pues, sea $f : \mathbb{N}^m \to \mathbb{N}$ una función de m-variables sobre los números naturales. Decimos que una fórmula φ, donde $v_1, \ldots, v_{m+1}$ son las únicas variables libres, *representa funcionalmente* a f (en la teoría $\mathrm{Cn} A_E$) sii para toda $a_1, \ldots, a_m$ en $\mathbb{N}$,

$$A_E \vdash \forall v_{m+1} [\varphi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}, v_{m+1}) \leftrightarrow v_{m+1} = \mathbf{S}^{f(a_1, \ldots, a_m)}\mathbf{0}].$$

(Nótese que la mitad "$\leftarrow$" de este enunciado es equivalente a $\varphi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}, \mathbf{S}^{f(a_1, \ldots, a_m)}\mathbf{0})$. La otra mitad "$\to$" agrega la unicidad.)

Teorema 33J Si φ representa funcionalmente a f en $\mathrm{Cn}\, A_E$, entonces también representa a f (como relación) en $\mathrm{Cn} A_E$.

Demostración para el caso en que $m = 1$. Como φ representa funcionalmente a f, entonces, para toda b:

$$A_E \vdash \varphi(\mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0}) \leftrightarrow \mathbf{S}^b\mathbf{0} = \mathbf{S}^{f(a)}\mathbf{0}.$$

Si $\langle a, b\rangle \in f$, es decir, si $f(a) = b$, entonces el lado derecho de esta doble implicación es válida y tenemos que

$$A_E \vdash \varphi(\mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0}).$$

En caso contrario, tenemos entonces que el lado derecho del bicondicional es refutable a partir de A_E (es decir, su negación es deducible) y entonces

$$A_E \vdash \neg \varphi(\mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0}). \qquad \dashv$$

El inverso de este teorema es falso; sin embargo, podemos hacer un cambio en la fórmula:

Teorema 33K Sea f una función sobre $\mathbb{N}$ representable (como relación) en $\mathrm{Cn}\, A_E$. Entonces podemos encontrar una fórmula φ que represente funcionalmente a f en $\mathrm{Cn}\, A_E$.

Demostración Para simplificar la notación supondremos que f es una función de una variable sobre $\mathbb{N}$. El enunciado deseado,

$$\forall v_2 \left[\varphi(\mathbf{S}^a\mathbf{0}, v_2) \leftrightarrow v_2 = \mathbf{S}^{f(a)}\mathbf{0}\right],$$

es equivalente a la conjunción de los siguientes dos enunciados

$$\varphi(\mathbf{S}^a\mathbf{0}, \mathbf{S}^{f(a)}\mathbf{0}) \tag{1}$$

y

$$\forall v_2[\varphi(\mathbf{S}^a\mathbf{0}, v_2) \rightarrow v_2 = \mathbf{S}^{f(a)}\mathbf{0}]. \tag{2}$$

El enunciado (1) es teorema de A_E siempre que φ represente a f. El enunciado (2) se refiere a la unicidad. Debemos construir φ de tal modo que este enunciado también sea teorema de A_E.

Sea θ una fórmula que represente a f (como relación binaria) y sea φ

$$\theta(v_1,v_2) \wedge \forall z\,(z < v_2 \rightarrow \neg\theta(v_1,z)).$$

Entonces podemos reescribir (2) de la siguiente manera:

$$\begin{aligned} \forall v_2[\theta(\mathbf{S}^a\mathbf{0}, v_2) \wedge \forall z\,(z < v_2 \rightarrow \neg\theta(\mathbf{S}^a\mathbf{0}, z)) \\ \rightarrow v_2 = \mathbf{S}^{f(a)}\mathbf{0}]. \end{aligned} \tag{2'}$$

Para demostrar que esto es un teorema de A_E, está claro que basta demostrar que

$$A_E \cup \{\theta(\mathbf{S}^a\mathbf{0}, v_2),\ \forall z\,(z < v_2 \rightarrow \neg\theta(\mathbf{S}^a\mathbf{0}, z))\} \vdash v_2 = \mathbf{S}^{f(a)}\mathbf{0}.$$

Llamemos Γ a este conjunto de hipótesis (a la izquierda de "$\vdash$"). Puesto que L3 $\in A_E$, basta demostrar que:

$$\Gamma \vdash v_2 \not< \mathbf{S}^{f(a)}0 \tag{3}$$

y

$$\Gamma \vdash \mathbf{S}^{f(a)}0 \not< v_2. \tag{4}$$

Obtener (4) es muy fácil, pues el último miembro de Γ nos garantiza que

$$\mathbf{S}^{f(a)}0 < v_2 \rightarrow \neg\,\theta(\mathbf{S}^a 0, \mathbf{S}^{f(a)}0)$$

y nosotros sabemos que

$$A_E \vdash \theta(\mathbf{S}^a 0, \mathbf{S}^{f(a)}0). \tag{5}$$

Para obtener (3) primero hay que observar que de A_E se desprenden los siguientes teoremas,

$$v_2 < \mathbf{S}^{f(a)}0 \leftrightarrow v_2 = \mathbf{S}^0 0 \vee \cdots \vee v_2 = \mathbf{S}^{f(a)-1}0 \tag{6}$$

y

$$\neg\,\theta(\mathbf{S}^a 0, \mathbf{S}^b 0) \quad \text{para } b = 0, \ldots, f(a) - 1. \tag{7}$$

Las fórmulas (6) y (7) implican la fórmula

$$v_2 < \mathbf{S}^{f(a)}0 \rightarrow \neg\,\theta(\mathbf{S}^a 0, v_2). \tag{8}$$

Pero como $\theta(\mathbf{S}^a 0, v_2) \in \Gamma$, entonces tenemos (3).

Esto demuestra que (2) es un teorema de A_E; (5) y (8) demuestran que (1) también es teorema de A_E. ⊣

Lo siguiente es demostrar que algunas funciones básicas son representables (en $\text{Cn}A_E$) y que la clase de las funciones representables es cerrada bajo ciertas operaciones entre funciones. A lo largo de esta sección nos referiremos a las funciones o relaciones representables en la teoría $\text{Cn}A_E$ simplemente como funciones o relaciones representables, omitiendo, por lo general, la frase "en la teoría $\text{Cn}A_E$".

En los casos más sencillos, una función m-aria puede ser representada por una ecuación:

$$v_{m+1} = t.$$

En realidad, cualquier ecuación de este tipo define en $\mathfrak{N}$ una función m-aria f, siempre y cuando las variables de t estén entre las variables $v_1, \ldots, v_m$. (El valor de f en $\langle a_1, \ldots, a_m \rangle$ es el número asignado a t en $\mathfrak{N}$, cuando a v_i se le asigna a_i, $1 \leq i \leq m$.) Además, sabemos que toda ecuación está numeralmente determinada por A_E, por lo que la ecuación representa a f como relación. De hecho, incluso representa funcionalmente a f, pues el enunciado

$$\forall v_{m+1}[v_{m+1} = t(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}) \leftrightarrow v_{m+1} = \mathbf{S}^{f(a_1, \ldots, a_m)}\mathbf{0}]$$

es lógicamente equivalente a

$$t(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}) = \mathbf{S}^{f(a_1, \ldots, a_m)}\mathbf{0},$$

que es un enunciado sin cuantificadores verdadero en $\mathfrak{N}$. (En este caso, $t(u_1, \ldots, u_m)$ es el término que se obtiene al sustituir v_1 por u_1, v_2 por u_2, etc.) Por ejemplo:

1. La función sucesor está (funcionalmente) representada por la ecuación

$$v_2 = \mathbf{S}v_1$$

2. Toda función constante es representable. La función m-aria cuyo valor constante es b está representada por la ecuación

$$v_{m+1} = \mathbf{S}^b\mathbf{0}.$$

3. La función proyección (con $1 \leq i \leq m$)

$$I_i^m(a_1, \ldots, a_m) = a_i$$

está representada por la ecuación

$$v_{m+1} = v_i.$$

4. La suma, el producto y la exponenciación están representadas por las ecuaciones

$$v_3 = v_1 + v_2,$$
$$v_3 = v_1 \cdot v_2,$$
$$v_3 = v_1 \mathbf{E}\, v_2,$$

respectivamente.

Estos ejemplos no deben engañar al lector, pues no toda función es representable mediante una ecuación.

Lo siguiente será demostrar que la familia de las funciones representables es cerrada bajo composición. Para simplificar la notación, supondremos que f es una función de una variable en $\mathbb{N}$ tal que

$$f(a) = g(h_1(a), h_2(a)).$$

Supongamos que g está funcionalmente representada por ψ y h_i por θ_i. Entonces, para representar f parece razonable tomar o bien

$$\forall y_1 \forall y_2(\theta_1(v_1, y_1) \to \theta_2(v_1, y_2) \to \psi(y_1, y_2, v_2))$$

o bien

$$\exists y_1 \exists y_2(\theta_1(v_1, y_1) \wedge \theta_2(v_1, y_2) \wedge \psi(y_1, y_2, v_2)).$$

(Piense que $\psi(y_1, y_2, v_2)$ es la fórmula que dice "$g(y_1, y_2) = v_2$" y piense también que $\theta_i(v_1, y_i)$ es la fórmula que dice "$h_i(v_1) = y_i$". Por lo tanto, la primera fórmula se puede traducir como "Para toda y_1, y_2, si $h_1(v_1) = y_1$ y $h_2(v_1) = y_2$, entonces $g(y_1, y_2) = v_2$." La segunda fórmula se traduce como "Existen y_1, y_2 tales que $h_1(v_1) = y_1$ y $h_2(v_1) = y_2$ y $g(y_1, y_2) = v_2$." Cualquiera de las dos sirve para decir que "$g(h_1(v_1), h_2(v_1)) = v_2$". Nótese que se tienen dos opciones, porque cuando algo es único, se puede anteponer indistintamente uno u otro cuantificador.)

Cualquiera de estas dos fórmulas funciona para representar a f. Digamos que φ es

$$\forall y_1 \forall y_2(\theta_1(v_1, y_1) \to \theta_2(v_1, y_2) \to \psi(y_1, y_2, v_2)).$$

Tomemos un número natural a; entonces tenemos

$$\forall v_2[\psi(\mathbf{S}^{h_1(a)}\mathbf{0}, \mathbf{S}^{h_2(a)}\mathbf{0}, v_2) \leftrightarrow v_2 = \mathbf{S}^{f(a)}\mathbf{0}]. \qquad (1)$$

$$\forall y_1[\theta_1(\mathbf{S}^a\mathbf{0}, y_1) \leftrightarrow y_1 = \mathbf{S}^{h_1(a)}\mathbf{0}]. \qquad (2)$$

$$\forall y_2[\theta_2(\mathbf{S}^a\mathbf{0}, y_2) \leftrightarrow y_2 = \mathbf{S}^{h_2(a)}\mathbf{0}]. \qquad (3)$$

Nosotros quisiéramos tener

$$\forall v_2(\varphi(\mathbf{S}^a\mathbf{0}, v_2) \leftrightarrow v_2 = \mathbf{S}^{f(a)}\mathbf{0}), \qquad (4)$$

es decir,

$$\forall v_2(\forall y_1 \forall y_2[\theta_1(\mathbf{S}^a\mathbf{0}, y_1) \rightarrow \theta_2(\mathbf{S}^a\mathbf{0}, y_2) \rightarrow \psi(y_1, y_2, v_2)] \leftrightarrow v_2 = \mathbf{S}^{f(a)}\mathbf{0}). \qquad (4)$$

Pero (1), (2) y (3) implican (4). En el ejercicio 4 se pide al lector que lo verifique.

El siguiente teorema generaliza esto.

Teorema 33L Sea g una función de n variables, sean $h_1, \ldots, h_n$ funciones de m variables y f una función definida de la siguiente manera:

$$f(a_1, \ldots, a_m) = g(h_1(a_1, \ldots, a_m), \ldots, h_n(a_1, \ldots, a_m)).$$

A partir de fórmulas que representen funcionalmente a g y $h_1, \ldots, h_n$, podemos encontrar una fórmula que represente funcionalmente a f.

La prueba que presentamos antes se refiere tan sólo al caso en el que $m = 1$ y $n = 2$. Sin embargo, el caso general se prueba exactamente de la misma manera.

Para el caso en que tengamos una función del tipo

$$f(a, b) = g(h(a), b),$$

basta notar que

$$f(a, b) = g(h(I_1^2(a, b)), I_2^2(a, b)).$$

Se puede aplicar el teorema anterior dos veces para demostrar que f es representable (suponiendo, claro está, que g y h lo son).

Para simplificar la discusión sobre funciones con un número arbitrario de variables, utilizaremos la notación vectorial. Por ejemplo, la ecuación del teorema anterior puede escribirse como

$$f(\vec{a}) = g(h_1(\vec{a}), \ldots, h_n(\vec{a})).$$

Otra propiedad de cerradura importante de la clase de las funciones representables en $\mathrm{Cn}\, A_E$ es que también es cerrada bajo el operador "mínimo cero".

Teorema 33M Supongamos que la función g de $(m + 1)$ variables es representable y que para toda $a_1, \ldots, a_m$ existe una b tal que

$$g(a_1, \ldots, a_m, b) = 0.$$

Entonces podemos encontrar una fórmula que represente a la función m-aria f, tal que

$$f(a_1, \ldots, a_m) = \text{la mínima } b \text{ tal que } g(a_1, \ldots, a_m, b) = 0.$$

(Esta última ecuación podría escribirse usando notación vectorial:

$$f(\vec{a}) = \text{la mínima } b \text{ tal que } g(\vec{a}, b) = 0.$$

La notación convencional para el operador mínimo cero es

$$f(\vec{a}) = \mu b\,[g(\vec{a}, b) = 0]$$

y a tal operador generalmente se lo conoce como el "operador μ".)

Demostración Tomaremos $m = 1$ para simplificar la notación; entonces

$$f(a) = b \quad \text{sii } g(a, b) = 0 \quad \text{y para toda} \quad c < b,\ g(a, c) \neq 0.$$

Si ψ representa a g, entonces podemos obtener una fórmula que represente a f (como relación) simplemente formalizando el lado derecho de la equivalencia anterior:

$$\psi(v_1, v_2, \mathbf{0}) \wedge \forall y\, (y < v_2 \to \neg \psi(v_1, y, \mathbf{0})).$$

Esta fórmula define (la gráfica de) f y está determinada numeralmente por A_E. ⊣

Un catálogo

Ahora construiremos un repertorio de funciones y relaciones representables (en Cn A_E) que incluirá, en particular, funciones para codificar y decodificar sucesiones de números.

0. Como consecuencia del teorema 33I, toda relación que tenga (en $\mathfrak{N}$) una definición sin cuantificadores es representable. También sabemos que la clase de las relaciones representables es cerrada bajo uniones, intersecciones y complementos. Por otro lado, si R es representable, entonces también lo son

$$\{\langle a_1, \ldots, a_m, b\rangle \mid \text{para toda } c < b,\ \langle a_1, \ldots, a_m, c\rangle \in R\}$$

y

$$\{\langle a_1, \ldots, a_m, b\rangle \mid \text{para alguna } c < b,\ \langle a_1, \ldots, a_m, c\rangle \in R\}.$$

Por ejemplo, toda relación finita tiene una definición sin cuantificadores, al igual que la relación de orden.

1. Una relación R es representable sii su función característica K_R lo es. (K_R es la función tal que si $\vec{a} \in R$, entonces $K_R(\vec{a}) = 1$ y, si no, entonces $K_R(\vec{a}) = 0$.)

Demostración ($\Leftarrow$) Supongamos que R es una relación unaria (es decir, un subconjunto de $\mathbb{N}$) y que K_R está representada por $\psi(v_1, v_2)$. Afirmamos que $\psi(v_1, \mathbf{S0})$ representa a R, pues define a R y está numeralmente determinada por A_E.

($\Rightarrow$) Supongamos que $\varphi(v_1)$ representa a R. Entonces

$$(\varphi(v_1) \wedge v_2 = \mathbf{S0}) \vee (\neg\varphi(v_1) \wedge v_2 = \mathbf{0})$$

representa a (la gráfica de) K_R por la misma razón expuesta en el párrafo anterior. (De hecho, esta fórmula incluso representa funcionalmente a K_R, como el lector puede comprobarlo.) ⊣

2. Si R es una relación binaria representable y f, g son funciones representables, entonces

$$\{\vec{a} \mid \langle f(\vec{a}), g(\vec{a})\rangle \in R\}$$

es representable. Esto también se cumple para una relación m-aria R y funciones $f_1, \ldots, f_m$.

Demostración Su función característica evaluada en $\vec{a}$ es igual a $K_R(f(\vec{a}), g(\vec{a}))$. Por lo tanto, se obtiene por composición a partir de funciones representables. ⊣

Por ejemplo, supongamos que R es una relación ternaria representable. Entonces

$$\{\langle x,y\rangle \mid \langle y,x,x\rangle \in R\}$$

es representable, ya que se puede ver como

$$\{\langle x,y\rangle \mid \langle I_2^2(x,y), I_1^2(x,y), I_1^2(x,y)\rangle \in R\}.$$

Vemos, entonces, que una relación representable se puede describir repitiendo y reordenando las variables.

3. Si R es una relación binaria representable, entonces también lo es

$$P = \{\langle a,b\rangle \mid \text{para alguna } c \leq b, \langle a,c\rangle \in R\}.$$

Demostración A partir del inciso 0 de nuestro catálogo tenemos que si

$$Q = \{\langle a,b\rangle \mid \text{para alguna } c < b, \langle a,c\rangle \in R\},$$

entonces Q es representable. Por otro lado,

$$\begin{aligned}\langle a,b\rangle \in P &\Leftrightarrow \langle a, S(b)\rangle \in Q\\ &\Leftrightarrow \langle I_1^2(a,b), S(I_2^2(a,b))\rangle \in Q.\end{aligned}$$

Así que, por el inciso 2 de nuestro catálogo, tenemos que P es representable. ⊣

Más generalmente, si R es una relación representable $(m+1)$-aria, entonces

$$\{\langle a_1,\ldots,a_m,b\rangle \mid \text{para alguna } c \leq b, \langle a_1,\ldots,a_m,c\rangle \in R\}$$

también es representable. En notación vectorial, esta relación sería

$$\{\langle \vec{a},b\rangle \mid \text{para alguna } c \leq b, \langle \vec{a},c\rangle \in R\}.$$

De manera análoga tenemos que

$$\{\langle \vec{a}, b\rangle \mid \text{para toda } c \leq b, \langle \vec{a}, c\rangle \in R\}$$

es representable.

4. La relación de divisibilidad

$$\{\langle a, b\rangle \mid a \text{ divide a } b \text{ en } \mathbb{N}\}$$

es representable.

Demostración a divide a b sii existe q tal que $q \leq b$ y $a \cdot q = b$. Como $\{\langle a, b, q\rangle \mid a \cdot q = b\}$ tiene una definición sin cuantificadores, entonces es representable. Recurriendo a los incisos ya expuestos en nuestro catálogo, podemos llegar a que la relación de divisibilidad es representable. (En particular, del inciso 3 del catálogo tenemos la representabilidad de

$$R = \{\langle a, b, c\rangle \mid \text{para alguna } q \leq c, a \cdot q = b\}$$

donde a divide a b sii $\langle a, b, b\rangle \in R$.) ⊣

5. El conjunto de los números primos es representable.

6. El conjunto de los pares de primos consecutivos es representable.

Demostración $\langle a, b\rangle$ es un par de primos consecutivos sii a es primo, b es primo, $a < b$ y no existe un primo c tal que $a < c$ y $c < b$. La parte derecha de esta equivalencia se puede formalizar mediante una fórmula numeralmente determinada. ⊣

Nótese (pues esto será importante en la sección 8 de este capítulo) que hasta ahora no hemos usado el hecho de que la exponenciación es representable.

Conforme avanzamos en la construcción del catálogo queda claro que lo que en realidad estamos haciendo es construir un "lenguaje" $\mathcal{L}$ que nos garantice que cualquier cosa (una función, una relación) que sea $\mathcal{L}$-definible (en $\mathfrak{N}$) será representable en nuestra teoría. Así que el teorema 33I nos dice que (a) las

fórmulas atómicas están permitidas en $\mathcal{L}$, (b) los conectivos están permitidos, y (c) se pueden usar los cuantificadores acotados. (En general, los cuantificadores no acotados no están permitidos.) Nuestro catálogo va introduciendo gradualmente, en el lenguaje $\mathcal{L}$, nuevos símbolos de predicado y de función. Por ejemplo, el inciso 6 del catálogo introduce el símbolo de predicado binario "consecutividad de primos", y el inciso 7 introducirá un símbolo de función para la función "enumeración de los primos". El uso de estos símbolos de función dentro de las expresiones del lenguaje $\mathcal{L}$ está justificado por el teorema 33L.

7. La función cuyo valor en a es p_a, el primo $(a + 1)$-ésimo, es representable. (Así, $p_0 = 2$, $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, $p_4 = 11$, y así sucesivamente.)

Demostración $p_a = b$ sii b es primo y existe una $c \leq b^{a^2}$ tal que (i)-(iii) son válidos:

(i) 2 no divide a c.

(ii) Para toda $q < b$ y $r \leq b$, si $\langle q, r\rangle$ es un par de primos consecutivos, entonces para toda $j < c$,

$$q^j \text{ divide a } c \iff r^{j+1} \text{ divide a } c.$$

(iii) b^a divide a c y b^{a+1} no.

Esta equivalencia no es obvia, pero al menos está claro que la relación definida por la parte derecha es representable. Para comprobar que la equivalencia es cierta, conviene primero notar que si $p_a = b$, entonces podemos tomar

$$c = 2^0 \cdot 3^1 \cdot 5^2 \cdot \ldots \cdot p_a^a.$$

Es fácil verificar que este valor de c cumple todas las condiciones. A la inversa, supongamos que c es un número que cumple las condiciones (i)-(iii). Afirmamos que c debe ser

$$2^0 \cdot 3^1 \cdot \ldots \cdot b^a \cdot \text{la potencia de primos más grandes.}$$

Por (i) está claro que el exponente de 2 en c es 0. Para los exponentes de los primos entre 2 y b podemos basarnos

en (ii). Por (iii), el exponente de b es a, así que b debe ser el $(a + 1)$-ésimo primo, p_a. ⊣

Esta función será muy útil para codificar sucesiones finitas de números por medio de un solo número. Sea

$$\langle a_0, \ldots, a_m \rangle = p_0^{a_0+1} \cdots p_m^{a_m+1}$$
$$= \prod_{i \leq m} p_i^{a_i+1}.$$

Esto también es válido para $m = -1$. Definimos $\langle\ \rangle = 1$. Por ejemplo,

$$\langle 2, 1 \rangle = 2^3 \cdot 3^2 = 72.$$

La idea es que 72 codifica únicamente el par $\langle 2, 1 \rangle$.

Existen otras maneras de codificar pares de números y sucesiones finitas de números. En la sección 8 de este capítulo usaremos la función de pareo

$$J(a, b) = \frac{1}{2}[(a + b)^2 + 3a + b],$$

que tiene la ventaja de crecer polinomialmente, a diferencia de $2^{a+1}3^{b+1}$, cuyo crecimiento es considerablemente más rápido. A continuación daremos una forma muy distinta de codificar, por ejemplo, los números 24, 117, 11 (en ese orden). Primero los convertimos a numerales de base 9: 26, 140, 12. Después, concatenamos estos numerales, intercalando nueves entre ellos: 269140912. La terna queda entonces codificada por el número (de base 10) 269,140,912. Este método podrá parecer extraño, pero produce un resultado *bastante* más pequeño que $2^{25}3^{118}5^{12}$, que tiene 73 dígitos en base 10.

8. Para toda m, la función cuyo valor en $a_0, \ldots, a_m$ es $\langle a_0, \ldots, a_m \rangle$ es representable.

9. Existe una función representable (cuyo valor en $\langle a, b \rangle$ se escribe como $(a)_b$) tal que para $b \leq m$,

$$(\langle a_0, \ldots, a_m \rangle)_b = a_b.$$

(Ésta será nuestra función "decodificadora". Por ejemplo, $(72)_0 = 2$ y $(72)_1 = 1$.)

Demostración Definimos $(a)_b$ como la mínima n tal que $a = 0$ o p_b^{n+2} no divide a a. (Siempre *hay* una n que cumple eso.) Observe que $(0)_b = 0$ y que para $a \neq 0$, $(a)_b$ es el exponente de p_b menos uno, en la factorización de a (pero no es menor que 0). Por lo tanto, para $b \leq m$,

$$(\langle a_0, \ldots, a_m \rangle)_b = a_b.$$

Para probar la representabilidad, usamos el operador mínimo cero. Sea

$$R = \{\langle a,b,n \rangle \mid a = 0 \quad \text{o} \quad p_b^{n+2} \text{ no divide a } a\}.$$

Entonces $(a)_b = \mu n\,[K_{\overline{R}}(a, b, n) = 0]$, donde $\overline{R}$ es el complemento de R. ⊣

Puesto que el método que se usó para esta prueba será de gran utilidad más adelante, lo enunciaremos como un teorema en sí mismo:

Teorema 33N Supongamos que R es una relación representable tal que para toda $\vec{a}$ existe n tal que $\langle \vec{a}, n \rangle \in R$. Entonces la función f definida por

$$f(\vec{a}) = \text{la mínima } n \text{ tal que } \langle \vec{a}, n \rangle \in R$$

es representable.

Demostración $f(\vec{a}) = \mu n\,[K_{\overline{R}}(\vec{a}, n) = 0]$. ⊣

Más adelante utilizaremos la notación

$$f(\vec{a}) = \mu n[\langle \vec{a}, n \rangle \in R].$$

10. Diremos que b es un *número de sucesión* sii para alguna $m \geq -1$ y algunas $a_0, \ldots, a_m$,

$$b = \langle a_0, \ldots, a_m \rangle.$$

(Para el caso en que $m = -1$ tenemos $\langle\ \rangle = 1$.) Entonces el conjunto de los números de sucesión es representable.

Demostración Ejercicio 5. ⊣

11. Existe una función representable lh tal que

$$\text{lh}\,\langle a_0, \ldots, a_m\rangle = m + 1.$$

(En este caso, "lh" es una abreviatura de "length" (longitud). Por ejemplo, lh 72 = 2.)

Demostración Sea lh a la mínima n tal que $a = 0$ o que p_n no divide a a. La función definida de este modo cumple con lo requerido. ⊣

12. Existe una función representable (cuyo valor en $\langle a, b\rangle$ se conoce como la restricción de a a b y se escribe como $a \upharpoonright b$) tal que, para toda $b \leq m + 1$,

$$\langle a_0, \ldots, a_m\rangle \upharpoonright b = \langle a_0, \ldots, a_{b-1}\rangle.$$

Demostración Sea $a \upharpoonright b$ la mínima n tal que $a = 0$, o bien $n \neq 0$, y para toda $j < b$ y toda $k < a$

$$p_j^k \text{ divide a } a \Rightarrow p_j^k \text{ divide a } n.$$

La función definida así cumple lo requerido. ⊣

13. (Recursión primitiva) A una función f de $(k + 1)$ variables le asociamos otra función $\overline{f}$ tal que $\overline{f}(a, b_1, \ldots, b_k)$ codifica los valores de $f(j, b_1, \ldots, b_k)$ para toda $j < a$. De manera más precisa, sea

$$\overline{f}(a,\vec{b}) = \langle f(0,\vec{b}), \ldots, f(a-1,\vec{b})\rangle.$$

Por ejemplo, $\overline{f}(0,\vec{b}) = \langle\,\rangle = 1$ codifica los primeros cero valores de f. $\overline{f}(1,\vec{b}) = \langle f(0,\vec{b})\rangle$. En general, $\overline{f}(a,\vec{b})$ es un número o código de sucesión cuya longitud (lh) es a, que codifica los primeros a valores de f.

Supongamos ahora que tenemos una función g de $(k + 2)$ variables. Entonces existe una única función f que satisface lo siguiente:

$$f(a,\vec{b}) = g(\overline{f}(a,\vec{b}), a, \vec{b}).$$

Por ejemplo:

$$f(0,\vec{b}) = g(\langle\,\rangle, 0, \vec{b}),$$
$$f(1,\vec{b}) = g(\langle f(0,\vec{b})\rangle, 1, \vec{b}).$$

(Debería ser intuitivamente claro que dicha función existe y es única. Para demostrarlo podemos aplicar el teorema de recursión de la sección 4 del capítulo I, obtener primero $\overline{f}$ y extraer después f.)

Teorema 33P Sea g una función de $(k + 2)$ variables y sea f la única función de $(k + 1)$ variables tal que, para toda a y toda k-ada $\vec{b}$,

$$f(a,\vec{b}) = g(\overline{f}(a,\vec{b}),a,\vec{b}).$$

Si g es representable, entonces f también lo es.

Demostración Afirmamos primero que $\overline{f}$ es representable. Esto se sigue del hecho de que

$\overline{f}(a,\vec{b})$ = la mínima s tal que s es un número de sucesión de longitud a y para toda i menor que a, $(s)_i = g(s \upharpoonright i, i, \vec{b})$.

Entonces f es representable, ya que

$$f(a,\vec{b}) = g(\overline{f}(a,\vec{b}),a,\vec{b})$$

y las funciones del lado derecho son representables. ⊣

En realidad, la expresión "recursión primitiva" suele usarse para una versión más sencilla de esto, dada en el ejercicio 8.

14. Dada una función representable F, la función cuyo valor en $(a,\vec{b})$ es

$$\prod_{i<a} F(i,\vec{b})$$

también es representable. Lo mismo sucede si tomamos Σ en lugar de Π. (Si $a = 0$, apegándonos a la convención, tenemos que: el producto vacío —el producto de ningún número— es igual a 1 y la suma vacía es igual a 0.)

Demostración Llamemos G a dicha función. Entonces

$$G(0,\vec{b}) = 1,$$
$$G(a+1,\vec{b}) = F(a,\vec{b}) \cdot G(a,\vec{b}).$$

Use el ejercicio 8 para terminar la demostración. ⊣

15. Definimos la *concatenación* de a con b, $a * b$, como sigue:

$$a * b = a \cdot \prod_{i < \mathrm{lh}\, b} p_{i+\mathrm{lh}\, a}^{(b)_i + 1}.$$

Ésta es una función representable de a y b, y

$$\langle a_1, \ldots, a_m \rangle * \langle b_1, \ldots, b_n \rangle = \langle a_1, \ldots, a_m, b_1, \ldots, b_n \rangle.$$

La operación de concatenación tiene, además, la propiedad de ser asociativa sobre los números de sucesión.

16. También quisiéramos tener la operación "asterisco grande". Sea

$$*_{i<a} f(i) = f(0) * f(1) * \cdots * f(a-1).$$

Dada una función representable F, la función cuyo valor en $(a, \vec{b})$ es $*_{i<a} F(i, \vec{b})$ es representable.

Demostración $*_{i<0} F(i, \vec{b}) = \langle\ \rangle = 1$ y

$$*_{i<a+1} F(i, \vec{b}) = *_{i<a} F(i, \vec{b}) * F(a, \vec{b}).$$

Pero esto es exactamente como el inciso 14 de nuestro catálogo. ⊣

Ejercicios

1. Demuestre que en la estructura $(\mathbb{N}; \cdot, E)$ se puede definir la relación de suma $\{(m, n, m+n) \mid m, n \in \mathbb{N}\}$. Concluya que el $\{0\}$, la relación de orden $<$ y la relación sucesor $\{(n, S(n)) \mid n \in \mathbb{N}\}$ son definibles en dicha estructura. (*Observación*: Se puede tener una versión más fuerte de este resultado sustituyendo simplemente la estructura $(\mathbb{N}; \cdot, E)$ por $(\mathbb{N}; E)$, pues es posible definir la relación de multiplicación en esa estructura usando una de las leyes de exponentes: $(d^a)^b = d^{ab}$.)

2. Demuestre el teorema 33C, que afirma que todos los enunciados sin cuantificadores que son verdaderos (en $\mathfrak{N}$) son teoremas de A_E. (Véase el esquema de demostración que se sugiere después de enunciar el teorema.)

3. Una teoría T (en un lenguaje con $\mathbf{0}$ y $\mathbf{S}$) es *ω-completa* sii para toda fórmula φ y toda variable x, ocurre que si $\varphi^x_{\mathbf{S}^n\mathbf{0}}$ pertenece a T para todo número natural n, entonces $\forall x \varphi$ pertenece a T. Demuestre que si T es una teoría consistente y ω-completa en el lenguaje de $\mathfrak{N}$, y $A_E \subseteq T$, entonces $T = \text{Th}\,\mathfrak{N}$.

4. Pruebe que en la demostración que antecede al teorema 33L, el conjunto de fórmulas (1), (2) y (3) implica lógicamente a la fórmula (4).

5. Demuestre que el conjunto de números de sucesión es representable (inciso 10 del catálogo).

6. ¿Es el 3 un número de sucesión? ¿Cuál es valor de $\text{lh}\,3$? Encuentre $(1 * 3) * 6$ y $1 * (3 * 6)$.

7. Demuestre lo siguiente:

(a) $a + 1 < p_a$.

(b) $(b)_k \leq b$. La igualdad se cumple sii $b = 0$.

(c) $\text{lh}\,a \leq a$. La igualdad se cumple sii $a = 0$.

(d) $a \upharpoonright i \leq a$.

(e) $\text{lh}\,(a \upharpoonright i)$ es el menor entre i y $\text{lh}\,a$.

8. Sean g y h funciones representables, y supongamos que

$$f(0, b) = g(b),$$
$$f(a + 1, b) = h(f(a, b), a, b).$$

Demuestre que f es representable.

9. Demuestre que existe una función representable f tal que, para toda n y todas $a_0, \ldots, a_n$,

$$f(\langle a_0, \ldots, a_n \rangle) = a_n.$$

(Por ejemplo, $f(72) = 1$ y $f(750) = 2$.)

10. Sea R una relación representable y suponga que g y h son funciones representables. Demuestre que f, definida de

la siguiente manera,

$$f(\vec{a}) = \begin{cases} g(\vec{a}) & \text{si } \vec{a} \in R, \\ h(\vec{a}) & \text{si } \vec{a} \notin R \end{cases}$$

es representable.

11. (Recursión monótona) Sea R una relación binaria representable sobre $\mathbb{N}$. Sea C el menor subconjunto de $\mathbb{N}$ (es decir, la intersección de todos los subconjuntos) tal que para toda n y todas $a_0, \ldots, a_{n-1}, b$,

$$\langle\langle a_0, \ldots, a_{n-1}\rangle, b\rangle \in R \text{ y } a_i \in C \text{ (para toda } i < n) \Rightarrow b \in C.$$

Supongamos, además, que (1), para toda n y todas las $a_0, \ldots, a_{n-1}, b$,

$$\langle\langle a_0, \ldots, a_{n-1}\rangle, b\rangle \in R \Rightarrow a_i < b \text{ (para toda } i < n),$$

y (2) que existe una función representable f tal que para toda n, $a_0, \ldots, a_{n-1}, b$,

$$\langle\langle a_0, \ldots, a_{n-1}\rangle, b\rangle \in R \Rightarrow n < f(b)$$

Demuestre que C es representable. (De algún modo, C está generado por R. En general, $C \neq \emptyset$, porque si $\langle\langle\,\rangle, b\rangle \in R$, entonces $b \in C$.)

4. *Aritmetización de la sintaxis*

En esta sección pretendemos exponer dos resultados:

1. Que algunas afirmaciones sobre fórmulas pueden transformarse en afirmaciones sobre números naturales (al asignar números a las expresiones).
2. Que, en muchos casos, estas afirmaciones (en español) sobre números naturales pueden traducirse al lenguaje formal y que la teoría Cn A_E es lo suficientemente fuerte como para que esas traducciones puedan demostrarse a partir de ella.

Esto nos dará la posibilidad de construir fórmulas que, aunque hablen de resultados sobre números, indirectamente se refieran a afirmaciones con respecto a fórmulas (¡incluso con respecto a sí mismas!). En la sección 5 de este capítulo, esto nos servirá para obtener resultados sobre indefinibilidad e indecidibilidad.

Números de Gödel

Lo primero que haremos es asignar números a las expresiones del lenguaje formal. Recuérdese que los símbolos de nuestro lenguaje son los que se encuentran listados en la tabla IX.

Tabla IX

Parámetros	Símbolos lógicos
0. $\forall$	1. (
2. **0**	3.)
4. **S**	5. $\neg$
6. $<$	7. $\rightarrow$
8. $+$	9. $=$
10. $\cdot$	11. v_1
12. **E**	13. v_2, etc.

Existe una función h tal que a cada símbolo le asocia el número escrito a su izquierda. Por lo tanto, $h(\forall) = 0$, $h(\mathbf{0}) = 2$, y $h(v_i) = 9 + 2i$. Con el fin de que nuestros resultados sean más útiles y manejables, supondremos únicamente que tenemos un lenguaje con **0** y S que está ***recursivamente numerado***. Con esto queremos decir que tenemos una función inyectiva h de los parámetros de ese lenguaje en los números pares, tal que las siguientes dos relaciones

$$\{\langle k, m\rangle \mid k \text{ es el valor de } h \text{ asignado a algún parámetro de predicado de } m \text{ argumentos}\}$$

y

$$\{\langle k, m\rangle \mid k \text{ es el valor de } h \text{ asignado a algún símbolo de función de } m \text{ argumentos}\}$$

son representables en $\mathrm{Cn} A_E$. Está claro que en el caso del lenguaje de $\mathfrak{N}$ estos conjuntos son, de hecho, finitos. El primer conjunto es $\{\langle 6, 2\rangle\}$, y el segundo es

$$\{\langle 2,0\rangle, \langle 4,1\rangle, \langle 8,2\rangle, \langle 10,2\rangle, \langle 12,2\rangle\}.$$

Para el caso de los símbolos lógicos, definimos h como antes. De manera que, para todo símbolo lógico s, $h(s)$ es un número impar.

Para una expresión del lenguaje $\varepsilon = s_0 \cdots s_n$ definimos su *número de Gödel*, $\sharp(\varepsilon)$, como sigue:

$$\sharp(s_0 \cdots s_n) = \langle h(s_0), \ldots, h(s_n)\rangle.$$

Por ejemplo, si usamos nuestra función original h para el lenguaje de $\mathfrak{N}$, tenemos que

$$\begin{aligned} &\sharp(\exists v_3\, v_3 = 0) \\ &\quad = \sharp((\neg \forall v_3(\neg = v_3 0))) \\ &\quad = \langle 1,5,0,15,1,5,9,15,2,3,3\rangle \\ &\quad = 2^2 \cdot 3^6 \cdot 5^1 \cdot 7^{16} \cdot 11^2 \cdot 13^6 \cdot 17^{10} \cdot 19^{16} \cdot 23^3 \cdot \\ &\qquad 29^4 \cdot 31^4. \end{aligned}$$

Se trata de un número muy grande, como del orden de 1.3×10^{75}. A un conjunto Φ de expresiones, le asignamos el siguiente conjunto de números de Gödel:

$$\sharp\Phi = \{\sharp(\varepsilon) \mid \varepsilon \in \Phi\}.$$

A una sucesión $\langle \alpha_0, \ldots, \alpha_n\rangle$ de expresiones (como es el caso de una deducción), le asignamos el número

$$\mathcal{G}(\langle \alpha_0, \ldots, \alpha_n\rangle) = \langle \sharp\alpha_0, \ldots, \sharp\alpha_n\rangle.$$

Lo siguiente será demostrar que diversas relaciones y funciones vinculadas a los números de Gödel son representables en $\mathrm{Cn} A_E$ (y, por lo tanto, recursivas). Cuando digamos que una relación o función es representable (sin especificar en qué teoría), nos referiremos, como en el caso de la sección anterior, a que son representables en la teoría $\mathrm{Cn} A_E$.

Nos valdremos de algunas abreviaturas en el lenguaje que usamos (es decir, el español, aunque nuestro lenguaje difiera cada vez más de lo que comúnmente consideramos español). Escribiremos "hay un número a tal que" como "$\exists a$". En el mismo sentido "$\exists a, b < c$" significará "hay dos números a y b, ambos menores que c, tales que". Utilizaremos "$\forall$" de forma similar. En el capítulo II no nos habríamos atrevido a usar estas abreviaciones por miedo a que se creara una confusión entre el lenguaje formal y el metalenguaje (español); sin embargo, creemos que a estas alturas el lector ya está preparado para evitar esos errores.

1. El conjunto de los números de Gödel de las variables es representable.

Demostración Dicho conjunto es $\{a \mid (\exists b < a)\; a = \langle 11 + 2b \rangle\}$. Y de los resultados de la sección anterior se puede concluir que se trata de un conjunto representable. ⊣

2. El conjunto de los números de Gödel de términos es representable.

Demostración El conjunto de los términos se definió inductivamente y los términos se construyeron a partir de elementos con números de Gödel más pequeños. Veremos este caso con más detalle, pues se trata del argumento que se suele usar para las relaciones definidas inductivamente.

Sea f la función característica del conjunto de números de Gödel de los términos. A partir de la definición de "término" tenemos que

$$f(a) = \begin{cases} 1 & \text{si } a \text{ es el número de Gödel de una variable,} \\ 1 & \text{si } (\exists i < \square, \exists k < a)\,[i \text{ es un número de} \\ & \quad \text{sucesión y } (\forall j < \operatorname{lh} i)\; f((i)_j) = 1 \text{ y} \\ & \quad k \text{ es el valor asignado por } h \text{ a algún} \\ & \quad \text{símbolo de función de } (\operatorname{lh} i) \text{ argumentos y} \\ & \quad a = \langle k \rangle * *_{j < \operatorname{lh} i} (i)_j], \\ 0 & \text{en cualquier otro caso.} \end{cases}$$

Sin embargo, ¿qué se puede usar en lugar del símbolo "□" como cota superior de i? Antes de demostrar que f es representable, necesitamos dar una cota superior para i que dependa de a, de alguna manera representable.

Afirmamos que se puede tomar $i < a^{a\,\mathrm{lh}\,a}$. Para demostrar que esta cota funciona supondremos que $a = \sharp s t_1 \cdots t_n$ (donde s es un símbolo de función de n argumentos y $t_1, \ldots, t_n$ son términos). Entonces queremos tomar $i = \langle \sharp t_1, \ldots, \sharp t_n \rangle$. En términos de a, ¿cuán grande puede ser i? Tenemos las siguientes cotas:

$$
\begin{aligned}
i &= 2^{\sharp t_1 + 1} \cdots p_{n-1}^{\sharp t_n + 1} \\
&\leq 2^a \cdots p_{n-1}^a \\
&< 2^a \cdots p_{\mathrm{lh}\,a - 1}^a \quad \text{pues } n = \mathrm{lh}\, i < \mathrm{lh}\, a \\
&\leq a^a \cdots a^a \quad (\mathrm{lh}\, a \text{ veces}) \text{ pues} \\
&\qquad a = 2^{(a)_0 + 1} \cdots p_{\mathrm{lh}\,a - 1}^{(a)_{\mathrm{lh}\,a-1}+1} \geq p_{\mathrm{lh}\,a - 1} \\
&= (a^a)^{\mathrm{lh}\,a} = a^{a\,\mathrm{lh}\,a}.
\end{aligned}
$$

Así que en la ecuación anterior para f podemos sustituir □ por $a^{a\,\mathrm{lh}\,a}$.

El lado derecho de esta ecuación menciona a f misma; sin embargo, en realidad sólo hace referencia a $f((i)_j)$, con $(i)_j < a$. Esta propiedad nos permite usar recursión primitiva. $f(a) = g(\overline{f}(a), a)$, donde

$$
g(s,a) = \begin{cases}
1 & \text{si } a \text{ es el número de Gödel de una variable,} \\
1 & \text{si } (\exists i < a^{a\,\mathrm{lh}\,a}, \exists k < a)\,[i \text{ es un número} \\
 & \quad \text{de sucesión y } (\forall j < \mathrm{lh}\, i)\ (s)_{(i)_j} = 1 \text{ y} \\
 & \quad k \text{ es el valor asignado por } h \text{ a algún} \\
 & \quad \text{símbolo de función de } (\mathrm{lh}\, i) \text{ argumentos} \\
 & \quad \text{y } a = \langle k \rangle * *_{j < \mathrm{lh}\, i} \langle (i)_j \rangle], \\
0 & \text{en cualquier otro caso.}
\end{cases}
$$

Ya que si en esta ecuación tomamos s igual a $\overline{f}(a)$, entonces $(s)_{(i)_j} = f((i)_j)$ para $(i)_j < a$. Por el teorema 33P, f es representable si g lo es.

Falta demostrar que g es representable; pero esto se sigue inmediatamente de los resultados de la sección anterior. La idea es que la gráfica de g es la unión de tres relaciones que corresponden a cada una de las condiciones de la ecuación que acabamos de dar. Cada relación se obtiene a partir de igualdades y de otras relaciones representables mediante cuantificación acotada y sustitución de funciones representables. ⊣

3. El conjunto de los números de Gödel de las fórmulas atómicas es representable.

Demostración a es el número de Gödel de una fórmula atómica sii $(\exists i < a^{a \operatorname{lh} a}, \exists k < a)$ [i es un número de sucesión y $(\forall j < \operatorname{lh} i)(i)_j$ es el número de Gödel de un término y k es el valor asignado por h a algún símbolo de predicado de $(\operatorname{lh} i)$ argumentos y $a = \langle k \rangle * *_{j<\operatorname{lh} i}(i)_j$]. ⊣

4. El conjunto de números de Gödel de las fórmulas es representable.

Demostración Las fórmulas se definieron inductivamente. Sea f la función característica del conjunto de números de Gödel de las fórmulas, entonces

$$f(a) = \begin{cases} 1 & \text{si } a \text{ es el número de Gödel de una fórmula atómica,} \\ 1 & \text{si } (\exists i < a)\,[a = \langle h((),h(\neg)\rangle * i * \langle h())\rangle \text{ y } f(i) = 1], \\ 1 & \text{si } (\exists i, j < a)\,[a = \langle h(()\rangle * i * \langle h(\rightarrow)\rangle * j * \langle h())\rangle \text{ y } f(i) = f(j) = 1], \\ 1 & \text{si } (\exists i, j < a)\,[a = \langle h(\forall)\rangle * i * j \text{ e } i \text{ es el número de Gödel de una variable y } f(j) = 1], \\ 0 & \text{en cualquier otro caso.} \end{cases}$$

Por el mismo argumento que se usó para el conjunto de los números de Gödel de los términos se tiene la representabilidad de f. ⊣

5. Hay una función representable Sb tal que para un término o fórmula α, una variable x y un término t,

$$\mathrm{Sb}(\sharp\alpha, \sharp x, \sharp t) = \sharp\alpha_t^x.$$

Demostración Será necesario definir $\mathrm{Sb}(a,b,c)$ en términos de los valores $\mathrm{Sb}(i,b,c)$ con $i < a$. Como en el caso del inciso 2 de este catálogo (la función característica del conjunto de términos), podremos demostrar que $\overline{\mathrm{Sb}}$ y Sb son ambas representables.

La función Sb está descrita por las siguientes seis condiciones (i)-(vi):

(i) Si a es el número de Gödel de una variable y $a = b$, entonces

$$\mathrm{Sb}(a,b,c) = c.$$

(ii) Si $(\exists i < a^{a\,\mathrm{lh}\,a}, \exists k < a)$ [i es un número de sucesión y $(\forall j < \mathrm{lh}\, i)(i)_j$ es el número de Gödel de un término y k es el valor asignado por h a algún símbolo de función o de predicado de $(\mathrm{lh}\, i)$ argumentos y $a = \langle k \rangle * *_{j<\mathrm{lh}\, i}(i)_j$], entonces

$$\mathrm{Sb}(a,b,c) = \langle k \rangle * *_{j<\mathrm{lh}\, i}\mathrm{Sb}((i)_j,b,c)$$

para esos i y k.

(iii) Si $(\exists i < a)$ [i es el número de Gödel de una fórmula y $a = \langle h((), h(\neg)\rangle * i * \langle h())\rangle$], entonces

$$\mathrm{Sb}(a,b,c) = \langle h((), h(\neg)\rangle * \mathrm{Sb}(i,b,c) * \langle h())\rangle$$

para esa i.

(iv) Si $(\exists i, j < a)$ [i, j son números de Gödel de fórmulas y $a = \langle h(()\rangle * i * \langle h(\rightarrow)\rangle * j * \langle h())\rangle$], entonces

$$\mathrm{Sb}(a,b,c) = \langle h(()\rangle * \mathrm{Sb}(i,b,c) * \langle h(\rightarrow)\rangle * \mathrm{Sb}(j,b,c) * \langle h())\rangle$$

para tales i y j.

(v) Si $(\exists i, j < a)$ [i es el número de Gödel de una variable tal que $i \neq b$ y j es el número de Gödel de una fórmula y $a = \langle h(\forall)\rangle * i * j$], entonces

$$\mathrm{Sb}(a,b,c) = \langle h(\forall)\rangle * i * \mathrm{Sb}(j,b,c)$$

para tales i y j.

(vi) Si no se cumple ninguna de las condiciones para a y b de los casos anteriores (donde se ignoraba la ecuación para Sb (a, b, c)), entonces

$$\mathrm{Sb}(a,b,c) = a.$$

Así que la función Sb se obtiene mediante recursión primitiva

$$\mathrm{Sb}(a,b,c) = G\,(\overline{\mathrm{Sb}}(a,b,c),a,b,c),$$

donde G es una función de cuatro argumentos. La gráfica de G es la unión de seis relaciones, de cinco argumentos cada una,

$$G = R_1 \cup R_2 \cup R_3 \cup R_4 \cup R_5 \cup R_6,$$

que corresponden a cada uno de los seis casos antes descritos.

La primera de esas relaciones es:

$R_1 = \{\langle s, a, b, c, d\rangle \mid a$ es el número de Gödel de una variable, y $a = b$ y $d = c\}$.

La segunda es:

$R_2 = \{\langle s, a, b, c, d\rangle \mid (\exists i < a^{a\,\mathrm{lh}\,a}, \exists k < a)[i$ es un número de sucesión y $(\forall j < \mathrm{lh}\,i)(i)_j$ es el número de Gödel de un término y k es valor asignado por h a algún símbolo de función o de predicado de $(\mathrm{lh}\,i)$ argumentos y $a = \langle k\rangle * *_{j<\mathrm{lh}\,i}(i)_j$ y $d = \langle k\rangle * *_{j<\mathrm{lh}\,i}(s)_{(i)_j}]\}$

y el resto de las relaciones son también las versiones correspondientes de los casos que describen Sb.

Es necesario percatarse de que G es efectivamente una función, es decir, que a cada entrada le asigna un solo valor. Esto es así porque si a cumple una de las condiciones dadas, entonces no puede cumplir ninguna otra. Y

si, por ejemplo, a cae en el caso (ii), entonces sabemos, por la sección 3 del capítulo II, que los números i y k están determinados de manera única.

Por último, nos podemos valer de los métodos comunes para verificar que R_1-R_6 son representables, de modo que G es representable, $\overline{\mathrm{Sb}}$ es representable y finalmente Sb es representable. (¡La sustitución es una operación bastante complicada!) ⊣

6. La función cuyo valor en n es $\sharp(\mathbf{S}^n\mathbf{0})$ es representable.

Demostración Llamemos f a dicha función. Entonces

$$f(0) = \langle h(\mathbf{0})\rangle,$$
$$f(n+1) = \langle h(\mathbf{S})\rangle * f(n).$$

Utilice el ejercicio 8 de la sección previa para terminar la demostración. ⊣

7. Existe una relación representable Fr tal que, dados α, que es un término o una fórmula, y la variable x,

$$\langle \sharp\alpha, \sharp x\rangle \in \mathrm{Fr} \Leftrightarrow x \text{ ocurre libre en } \alpha.$$

Demostración $\langle a, b\rangle \in \mathrm{Fr} \Leftrightarrow \mathrm{Sb}(a, b, \sharp\mathbf{0}) \neq a.$ ⊣

8. El conjunto de números de Gödel de los enunciados es representable.

Demostración a es el número de Gödel de un enunciado sii a es el número de Gödel de una fórmula y para todo $b < a$, si b es el número de Gödel de una variable, entonces $\langle a, b\rangle \notin \mathrm{Fr}$. ⊣

9. Existe una relación representable Sbl tal que para toda fórmula α, toda variable x y todo término t, $\langle \sharp\alpha, \sharp x, \sharp t\rangle \in \mathrm{Sbl}$ sii t es sustituible por x en α.

Demostración Ejercicio 1. ⊣

10. La relación Gen, tal que $\langle a, b\rangle \in \mathrm{Gen}$ sii a es el número de Gödel de una fórmula y b es el número de Gödel de una generalización de esa fórmula, es representable.

Demostración $\langle a,b\rangle \in$ Gen sii $a = b$ o $(\exists i,j < b)[i$ es el número de Gödel de una variable y $\langle a,j\rangle \in$ Gen y $b = \langle (h(\forall)) * i * j]$. Aplique el argumento acostumbrado a la función característica de Gen. ⊣

11. El conjunto de los números de Gödel de las tautologías es representable.

El conjunto de las tautologías es intuitivamente decidible, pues podemos usar el método de las tablas de verdad. Para obtener la representabilidad, escribimos de nuevo las tablas de verdad en términos de números de Gödel. Para llegar a eso se necesitan algunos resultados preliminares:

11.1 La relación R, tal que $\langle a,b\rangle \in R$ sii a es el número de Gödel de una fórmula α y b es el número de Gödel de una componente prima de α, es representable.

Demostración $\langle a,b\rangle \in R \Leftrightarrow a$ es el número de Gödel de una fórmula y sucede alguno de los siguientes casos:

(i) $a = b$ y $(a)_0 \neq h(()$.
(ii) $(\exists i < a)[a = (h((), h(\neg)) * i * (h()))$ e $\langle i,b\rangle \in R]$.
(iii) El análogo a (ii) pero con $\rightarrow$.

Aplique el argumento usual a la función característica de R. ⊣

11.2 Existe una función representable P tal que, para toda fórmula α, $P(\sharp\alpha) = \langle \sharp\beta_1, \ldots, \sharp\beta_n\rangle$, la lista de números de Gödel de las componentes primas de α, en orden numérico.

Demostración Primero hay que definir una función g que nos dé la componente prima de $\natural a$ que sigue después de $\natural y$ (donde $\natural a$ es la fórmula α para la cual $a = \sharp\alpha$).

$g(a,y) =$ la mínima n tal que o bien $n = a + 1$ o bien sucede que $y < n$ y $\langle a,n\rangle \in R$.

Lo siguiente es definir una función h tal que $h(a,n)$ nos dé la $(n + 1)$-ésima componente prima de $\natural a$ (si es que hay tal cantidad de componentes primas):

$$h(a,0) = g(a,0) \qquad h(a,n+1) = g(a,h(a,n)).$$

Por último, sea $P(a) = *_{i<k}\langle h(a,i)\rangle$ donde k es el número más pequeño tal que $h(a,k) > a$. ⊣

11.3 Decimos que un entero v *codifica una asignación de verdad* para α sii v es un número de sucesión y $\operatorname{lh} v = \operatorname{lh} P(\sharp\alpha)$ y $(\forall i < \operatorname{lh} v)(\exists e < 2)(v)_i = \langle (P(\sharp\alpha))_i, e\rangle$. Se trata de una condición de representabilidad para v y $\sharp\alpha$.

Por ejemplo, si $P(\sharp\alpha) = \langle \sharp\beta_0, \ldots, \sharp\beta_n\rangle$, entonces:

$$v = \langle\langle \sharp\beta_0, e_0\rangle, \ldots, \langle \sharp\beta_n, e_n\rangle\rangle,$$

donde cada e_i es 0 o 1. Más adelante necesitaremos una cota superior para v en términos de $\sharp\alpha$. La v más grande se obtiene cuando cada e_i es igual a 1; también $\sharp\beta_i \leq \sharp\alpha$, así que

$$\begin{aligned} v &\leq \langle\langle \sharp\alpha, 1\rangle, \ldots, \langle \sharp\alpha, 1\rangle\rangle \\ &= *_{i<\operatorname{lh} P(\sharp\alpha)}\langle\langle \sharp\alpha, 1\rangle\rangle. \end{aligned}$$

11.4 Existe una relación representable Tr tal que para toda fórmula α y toda v que codifique una asignación de verdad para α (o más), $\langle \sharp\alpha, v\rangle \in \text{Tr}$ sii esa asignación de verdad satisface α.

Demostración Ejercicio 2. ⊣

Por último, α es una tautología sii α es una fórmula y para toda v que codifica una asignación de verdad para α, $\langle \sharp\alpha, v\rangle \in$ Tr. El cuantificador (en español) sobre v puede acotarse mediante una función representable de $\sharp\alpha$, como se explicó en 11.3.

12. El conjunto de los números de Gödel de las fórmulas de la forma $\forall x\, \varphi \to \varphi^x_t$, donde t es un término sustituible por x en φ, es representable.

Demostración α es una fórmula de este tipo sii ($\exists$ una fórmula $\varphi < \alpha$) ($\exists$ una variable $x < \alpha$) ($\exists$ un término $t < \alpha$) [t es sustituible por x en φ y $\alpha = \forall x\, \varphi \to \varphi^x_t$]. En este caso, por "$\varphi < \alpha$" queremos decir que $\sharp\varphi < \sharp\alpha$. Este bicondicional se puede reescribir en términos de números de Gödel: a pertenece al conjunto sii $(\exists f < a)(\exists x < a)(\exists t < a)$ [f es el número de Gödel de una

fórmula y x es el número de Gödel de una variable y t es el número de Gödel de un término y $\langle f, x, t\rangle \in \mathrm{Sb1}$ y

$$a = \langle h((), h(\forall)\rangle * x * f * \langle h(\rightarrow)\rangle * \mathrm{Sb}(f, x, t) * \langle h())\rangle\}. \quad \dashv$$

13. El conjunto de los números de Gödel de las fórmulas del tipo $\forall x(\alpha \rightarrow \beta) \rightarrow \forall x\, \alpha \rightarrow \forall x\, \beta$ es representable.

Demostración γ es una fórmula de este tipo sii ($\exists$ una variable $x < \gamma$) ($\exists$ fórmulas $\alpha, \beta < \gamma$) $[\gamma = \forall x(\alpha \rightarrow \beta) \rightarrow \forall x\, \alpha \rightarrow \forall x\, \beta]$. Es muy fácil reescribir esto en términos de números de Gödel, tal como se hizo en 12. $\dashv$

14. El conjunto de números de Gödel de las fórmulas del tipo $\alpha \rightarrow \forall x\, \alpha$, donde x no ocurre libre en α, es representable.

Demostración Similar a la demostración de 13. $\dashv$

15. El conjunto de los números de Gödel de las fórmulas del tipo $x = x$ es representable.

Demostración Similar a la demostración de 13. $\dashv$

16. El conjunto de los números de Gödel de las fórmulas del tipo $x = y \rightarrow \alpha \rightarrow \alpha'$, donde α es atómica y α' es el resultado de la sustitución de x por y en varios lugares o en ninguno de α, es representable.

Demostración Esta demostración también es similar a la de 13, excepto por la relación de "sustitución parcial". Sea $\langle a, b, x, y\rangle \in \mathrm{Psb}$ sii x, y son números de Gödel de variables, a es el número de Gödel de una fórmula atómica, b es un número de sucesión de longitud $\mathrm{lh}\, a$, y para toda $j < \mathrm{lh}\, a$, o bien $(a)_j = (b)_j$, o bien $(a)_j = x$ y $(b)_j = y$. Esta relación es representable. $\dashv$

17. El conjunto de los números de Gödel de axiomas lógicos es representable.

Demostración α es un axioma lógico sii $\exists \beta \leq \alpha$ tal que α es una generalización de β y β está en alguno de los conjuntos expuestos en 11-16. $\dashv$

18. Dado un conjunto finito de fórmulas A,

$$\{\mathcal{G}(D) \mid D \text{ es una deducción a partir de } A\}$$

es representable. De hecho, en este caso basta con que $\sharp A$ sea representable.

Demostración Un número d pertenece a este conjunto sii d es un número de sucesión de longitud positiva y para toda i menor que $\text{lh}\, d$ se cumple alguna de las siguientes condiciones:

1. $(d)_i \in \sharp A$,
2. $(d)_i$ es el número de Gödel de un axioma lógico, o
3. $(\exists j,k < i)[(d)_j = \langle h\,(()\rangle * (d)_k * \langle h(\rightarrow)\rangle * (d)_i * \langle h\,())\rangle]$.

Esto es representable siempre y cuando $\sharp A$ lo sea, lo que ciertamente sucede cuando A es finito. ⊣

19. Toda relación recursiva es representable en $\text{Cn}\, A_E$.

Demostración Recuérdese que una relación R es recursiva sii existe ***algún*** conjunto finito y consistente de enunciados A tal que alguna fórmula ρ representa R en $\text{Cn}A$. (Podemos suponer, sin pérdida de generalidad, que el lenguaje tiene sólo un número finito de parámetros: los que ocurren en el conjunto finito A, los que ocurren en ρ y $\mathbf{0}$, $\mathbf{S}$ y $\forall$.) Para el caso de una relación unaria R, tenemos que $a \in R$ sii la mínima D que es una deducción a partir de A de $\rho(\mathbf{S}^a\mathbf{0})$ o bien de $\neg\rho(\mathbf{S}^a\mathbf{0})$ es, de hecho, una deducción de $\rho(\mathbf{S}^a\mathbf{0})$.

De manera más formal, $a \in R$ sii el último componente de $f(a)$ es $\sharp\rho(\mathbf{S}^a\mathbf{0})$, donde

$f(a) =$ la mínima d tal que pertenece al conjunto dado en el inciso 18 y cuyo último componente es $\sharp\rho(\mathbf{S}^a\mathbf{0})$ o $\sharp\neg\rho(\mathbf{S}^a\mathbf{0})$.

Para esta ρ (fija), siempre existe dicha d. ⊣

Puesto que el inverso del inciso 19 es inmediato, tenemos el siguiente teorema:

Teorema 34A Una relación es recursiva sii es representable en la teoría $\text{Cn}\, A_E$.

A partir de este punto usaremos el término "recursivo" en lugar de "representable".

Corolario 34B Toda relación recursiva es definible en $\mathfrak{N}$.

20. Supongamos ahora que tenemos un conjunto de enunciados A tal que $\sharp A$ es recursivo. Entonces $\sharp \text{Cn} A$ *no* necesariamente es recursivo (como demostraremos en la siguiente sección); no obstante, tenemos una forma de definir $\text{Cn} A$ a partir de A:

$a \in \sharp \text{Cn} A$ sii $\exists d[d$ es el número de Gödel de una deducción a partir de A y el último componente de d es a y a es el número de Gödel de un enunciado$]$.

La parte que está entre corchetes es recursiva, por la demostración de 18. Sin embargo, en general no se puede dar una cota para el número d. Lo más que podemos decir es que $\sharp \text{Cn} A$ es el dominio de una relación recursiva (o, como diremos más adelante, que es *recursivamente numerable*).

El resultado del inciso 20 será fundamental para el desarrollo de nuestro trabajo posterior, así que más adelante se replanteará como el teorema 35I.

21. Si $\sharp A$ es recursivo y $\text{Cn} A$ es una teoría completa, entonces $\sharp \text{Cn} A$ es recursivo.

En otras palabras, una teoría recursivamente axiomatizable y completa es recursiva. Este resultado es análogo al corolario 25G, que establece que una teoría axiomatizable y completa es decidible.

La demostración es esencialmente la misma. Sea (en el caso de una teoría consistente)

$g(s) =$ la mínima d tal que s no es el número de Gödel de un enunciado, o d pertenece al conjunto expuesto en el inciso 18 y su última componente es o bien s, o bien $\langle h((), h(\neg)\rangle * s * \langle h())\rangle$.

Por lo tanto, $g(\sharp\sigma)$ es igual a $\mathcal{G}$ de la mínima deducción de σ o de $\neg\sigma$ a partir de A. Y $s \in \sharp \text{Cn} A$ sii $s > 0$ y la última componente de $g(s)$ es s. ⊣

Una vez que hemos llegado a este punto, podemos abrir nuevamente la discusión sobre la plausibilidad de la tesis de Church. Supongamos que la relación R es decidible. Entonces hay una lista finita de instrucciones explícitas (un programa) para el procedimiento de decisión. Muy probablemente el procedimiento consiste en una serie de pasos básicos o elementales que se repiten. (El lector familiarizado con la programación de computadoras sabe que incluso un programa corto puede requerir mucho tiempo para su ejecución, pero que algunos comandos básicos se utilizan una y otra vez.) En principio, todo paso básico es muy sencillo.

Mediante un método similar a la numeración de Gödel, podemos reflejar el procedimiento de decisión en los números enteros. Entonces la función característica de R puede escribirse de la siguiente manera:

$K_R(\vec{a}) = U$ [la mínima s, tal que

(i) $(s)_0$ codifica la entrada $\vec{a}$;

(ii) para toda $i <$ lh s positiva, $(s)_i$ se obtiene a partir de $(s)_{i-1}$ cuando se aplica el paso básico correspondiente;

(iii) el último componente de s describe el resultado final y, por lo tanto, indica que el procedimiento ha terminado],

donde U es una función que da una respuesta (afirmativa o negativa) a partir del último componente de s. Entonces, la recursividad de R se reduce a la recursividad de U y de las relaciones dadas en (i), (ii) y (iii). En algunos casos, como el de los procedimientos de decisión que se obtienen con las máquinas registradoras de la sección 6 de este capítulo, la recursividad de estos componentes se puede verificar muy fácilmente. Parece muy poco probable que un procedimiento de decisión se considere efectivo y que, no obstante, sus componentes no sean recursivos. Por ejemplo, en (ii) parece posible hacer que cada paso básico sea muy sencillo y, en particular, hacer que cada uno de ellos sea recursivo.

Ejercicios

1. Demuestre el inciso 9 de esta sección.

2. Demuestre el inciso 11.4 de esta sección.

3. Use el ejercicio 11 de la sección 3 de este capítulo para dar otra prueba de que el conjunto de los números de Gödel de términos es representable (inciso 2).

4. Sea T una teoría consistente y recursivamente axiomatizable (dentro de un lenguaje recursivamente numerado con $\mathbf{0}$ y $\mathbf{S}$). Demuestre que toda relación representable en T es recursiva.

5. *Incompletud e indecidibilidad*

En esta sección sacaremos provecho del trabajo realizado en las secciones 3 y 4 de este mismo capítulo. Hemos asignado números de Gödel a expresiones y hemos demostrado que ciertas relaciones intuitivamente decidibles sobre $\mathbb{N}$ (relacionadas con nociones sintácticas sobre expresiones) son representables en CnA_E.

A lo largo de esta sección tomaremos como lenguaje el de $\mathfrak{N}$. (La elección del lenguaje determina el significado de "Cn" y de "teoría".)

Lema del punto fijo Dada una fórmula β, en la que sólo v_1 ocurre libre, se puede encontrar un enunciado σ tal que

$$A_E \vdash [\sigma \leftrightarrow \beta(\mathbf{S}^{\sharp\sigma}\mathbf{0})].$$

Podemos pensar que σ dice indirectamente "β es verdadera con respecto a mí". Por supuesto que σ, en realidad, no dice nada: se trata tan sólo de una sucesión de símbolos. Incluso cuando se traduce al español, de acuerdo con la interpretación canónica de la estructura $\mathfrak{N}$, sólo se refiere a números, a sus sucesores, productos, etc. Es la asociación que hemos establecido entre números y expresiones la que nos permite pensar que σ se refiere a una fórmula, en este caso, a sí misma.

Demostración Supongamos que $\theta(v_1, v_2, v_3)$ representa funcionalmente, en Cn A_E, una función cuyo valor en $\langle \sharp\alpha, n\rangle$ es

$\sharp(\alpha(\mathbf{S}^n\mathbf{0}))$. (Revísense los incisos 5 y 6 de la sección 4 de este capítulo). Consideremos primero la fórmula

$$\forall v_3\,[\theta(v_1, v_1, v_3) \to \beta(v_3)]. \tag{1}$$

(Podríamos suponer que v_3 es sustituible por v_1 en β. La fórmula anterior sólo tiene a v_1 libre y define un conjunto en $\mathfrak{N}$ al que pertenece $\sharp\alpha$ sii $\sharp(\alpha(\mathbf{S}^{\sharp\alpha}\mathbf{0}))$ está en el conjunto definido por β.) Sea q el número de Gödel de (1) y sea σ

$$\forall v_3\,[\theta(\mathbf{S}^q\mathbf{0}, \mathbf{S}^q\mathbf{0}, v_3) \to \beta(v_3)].$$

Obtenemos σ al sustituir v_1 por $\mathbf{S}^q\mathbf{0}$ en (1). Nótese que σ nos asegura (bajo $\mathfrak{N}$) que $\sharp\sigma$ está en el conjunto definido por β. Sin embargo, es necesario verificar que

$$\sigma \leftrightarrow \beta(\mathbf{S}^{\sharp\sigma}\mathbf{0}) \tag{2}$$

es consecuencia de A_E. Puesto que θ representa funcionalmente una función cuyo valor en $\langle q, q\rangle$ es $\sharp\sigma$, tenemos que

$$A_E \vdash \forall v_3\,[\theta(\mathbf{S}^q\mathbf{0}, \mathbf{S}^q\mathbf{0}, v_3) \leftrightarrow v_3 = \mathbf{S}^{\sharp\sigma}\mathbf{0}]. \tag{3}$$

El bicondicional (2) se puede obtener de la siguiente manera:

($\to$) Está claro (considerando cómo es σ) que

$$\sigma \vdash \theta(\mathbf{S}^q\mathbf{0}, \mathbf{S}^q\mathbf{0}, \mathbf{S}^{\sharp\sigma}\mathbf{0}) \to \beta(\mathbf{S}^{\sharp\sigma}\mathbf{0}).$$

Y, por (3),

$$A_E \vdash \theta(\mathbf{S}^q\mathbf{0}, \mathbf{S}^q\mathbf{0}, \mathbf{S}^{\sharp\sigma}\mathbf{0}).$$

Por lo tanto,

$$A_E; \sigma \vdash \beta(\mathbf{S}^{\sharp\sigma}\mathbf{0}),$$

que nos da un lado del bicondicional (2).

($\leftarrow$) El enunciado (3) implica que

$$\beta(\mathbf{S}^{\sharp\sigma}\mathbf{0}) \to [\forall v_3(\theta(\mathbf{S}^q\mathbf{0}, \mathbf{S}^q\mathbf{0}, v_3) \to \beta(v_3))].$$

Pero la parte entre corchetes es justamente σ. ⊣

(A veces se usa $\ulcorner\sigma\urcorner$ para denotar $\mathbf{S}^{\sharp\sigma}\mathbf{0}$. Con esa notación, el lema del punto fijo nos dice que $A_E \vdash (\sigma \leftrightarrow \beta(\ulcorner\sigma\urcorner))$.)

Nuestra primera aplicación de este lema no está relacionada con la subteoría Cn A_E y sólo recurre al hecho más débil de que

$$\models_{\mathfrak{N}} [\sigma \leftrightarrow \beta(\mathbf{S}^{\sharp\sigma}\mathbf{0})].$$

Teorema de indefinibilidad de Tarski (1933) El conjunto $\sharp$Th $\mathfrak{N}$ no es definible en $\mathfrak{N}$.

Demostración Considere cualquier fórmula β (que piense que *pueda* definir a $\sharp$Th $\mathfrak{N}$). Por el lema del punto fijo (aplicado a $\neg\beta$) tenemos un enunciado σ tal que

$$\models_{\mathfrak{N}} [\sigma \leftrightarrow \neg\beta(\mathbf{S}^{\sharp\sigma}\mathbf{0})].$$

(Si β define a $\sharp$Th $\mathfrak{N}$, entonces σ dice indirectamente: "Soy falsa.") Entonces

$$\models_{\mathfrak{N}} \sigma \iff \not\models_{\mathfrak{N}} \beta(\mathbf{S}^{\sharp\sigma}\mathbf{0}),$$

de modo que o bien σ es verdadera pero (su número de Gödel) no está en el conjunto definido por β, o bien es falsa y pertenece a dicho conjunto. Cualquiera de los dos casos demuestra que β no puede definir a $\sharp$Th $\mathfrak{N}$. ⊣

De este teorema se desprende inmediatamente la indecidibilidad de la teoría de $\mathfrak{N}$:

Corolario 35A $\sharp$Th $\mathfrak{N}$ no es recursivo.

Demostración Todo conjunto recursivo es (por el corolario 34B) definible en $\mathfrak{N}$. ⊣

Teorema de incompletud de Gödel (1931) Si $A \subseteq$ Th $\mathfrak{N}$ y $\sharp A$ es recursivo, entonces Cn A no es una teoría completa.

Por lo tanto, no hay una axiomatización completa y recursiva de Th $\mathfrak{N}$.

Demostración Dado que $A \subseteq$ Th $\mathfrak{N}$, tenemos que Cn $A \subseteq$ Th $\mathfrak{N}$. Si CnA es una teoría completa, entonces se cum-

ple la igualdad. Por otro lado, si $\mathrm{Cn}\, A$ es una teoría completa, entonces $\sharp\mathrm{Cn}\, A$ es recursivo (inciso 21 de la sección anterior). Pero, por el corolario anterior, $\sharp\mathrm{Th}\, \mathfrak{N}$ no es recursivo. ⊣

En particular, tenemos que $\mathrm{Cn}\, A_E$ no es una teoría completa y, por lo tanto, no puede ser igual a $\mathrm{Th}\, \mathfrak{N}$. Además, no hay ningún conjunto recursivo de axiomas verdaderos que permita eliminar la incompletud. (Desde luego, cuando hablamos de un conjunto recursivo de enunciados nos referimos a un conjunto Σ tal que $\sharp\Sigma$ es recursivo.)

Podemos obtener más información a partir de la prueba del teorema de Gödel. Supongamos que tenemos en mente un conjunto recursivo $A \subseteq \mathrm{Th}\, \mathfrak{N}$. Entonces, por el inciso 20 de la sección 4 de este capítulo, podemos encontrar una fórmula β que defina a $\sharp\mathrm{Cn}\, A$ en $\mathfrak{N}$. El enunciado σ dado en la prueba del teorema de Tarski es (como se observó ahí) un enunciado verdadero que *no* está en $\mathrm{Cn}\, A$. Dicho enunciado establece que $\sharp\sigma$ no pertenece al conjunto definido por β y, por lo tanto, indirectamente nos dice: "No soy un teorema de A." Así que $A \nvdash \sigma$ y, por supuesto, $A \nvdash \neg\sigma$. Esta manera de ver la demostración es más cercana a la prueba original de Gödel, que no usó el teorema de Tarski. De hecho, la forma en la que Gödel enunció el teorema no involucra $\mathrm{Th}\, \mathfrak{N}$; nos hemos permitido cierta libertad al poner esta versión bajo su nombre.

Ahora daremos un lema que (en términos generales) nos garantiza la posibilidad de agregar un nuevo axioma (y, por lo tanto, un número finito de axiomas) a una teoría recursiva sin que se pierda la propiedad de recursividad.

Lema 35B Si $\sharp\mathrm{Cn}\, \Sigma$ es recursivo, entonces $\sharp\mathrm{Cn}\, (\Sigma; \tau)$ es recursivo.

Demostración $\alpha \in \mathrm{Cn}\, (\Sigma; \tau) \Leftrightarrow (\tau \to \alpha) \in \mathrm{Cn}\, \Sigma$. Por lo tanto,

$$a \in \sharp\mathrm{Cn}\, (\Sigma; \tau) \Longleftrightarrow a \text{ es el número de Gödel de un enunciado y } \langle h(()\rangle * \sharp\tau * \langle h(\to)\rangle * a * \langle h())\rangle \text{ está en } \sharp\mathrm{Cn}\, \Sigma.$$

Esto es recursivo por los resultados de las secciones anteriores. ⊣

Teorema 35C (Indecidibilidad fuerte de Cn A_E) Sea T una teoría tal que $T \cup A_E$ es consistente. Entonces, $\sharp T$ no es recursivo.

(Puesto que en esta sección hemos estado trabajando con el lenguaje de $\mathfrak{N}$, la palabra "teoría" significa aquí "teoría en el lenguaje de $\mathfrak{N}$".)

Demostración Sea T' la teoría Cn $(T \cup A_E)$. Si $\sharp T$ es recursivo, como A_E es finito, podemos concluir, por el lema anterior, que $\sharp T'$ también es recursivo.

Supongamos, entonces, que $\sharp T'$ es recursivo, así que está representado en Cn A_E por alguna fórmula β. Por el lema del punto fijo tenemos un enunciado σ tal que

$$A_E \vdash [\sigma \leftrightarrow \neg \beta(\mathbf{S}^{\sharp\sigma}\mathbf{0})]. \qquad (*)$$

(σ afirma indirectamente: "No pertenezco a T'.")

$$\begin{aligned} \sigma \notin T' &\Rightarrow \sharp\sigma \notin \sharp T' \\ &\Rightarrow A_E \vdash \neg \beta(\mathbf{S}^{\sharp\sigma}\mathbf{0}) \\ &\Rightarrow A_E \vdash \sigma \qquad \text{por } (*) \\ &\Rightarrow \sigma \in T'. \end{aligned}$$

Entonces $\sigma \in T'$. Pero esto no puede ser cierto, pues:

$$\begin{aligned} \sigma \in T' &\Rightarrow \sharp\sigma \in \sharp T' \\ &\Rightarrow A_E \vdash \beta(\mathbf{S}^{\sharp\sigma}\mathbf{0}) \\ &\Rightarrow A_E \vdash \neg \sigma \qquad \text{por } (*) \\ &\Rightarrow (\neg \sigma) \in T', \end{aligned}$$

lo cual contradice la consistencia de T'. ⊣

Corolario 35D Supongamos que $\sharp\Sigma$ es recursivo y $\Sigma \cup A_E$ consistente. Entonces, Cn Σ no es una teoría completa.

Demostración Una teoría recursivamente axiomatizable y completa es recursiva (inciso 21 de la sección 4 de este capítulo). Pero $\sharp$Cn Σ no es recursivo, por el teorema anterior. ⊣

Este corolario es otra versión del teorema de incompletud de Gödel, en la que se sustituyó la verdad en $\mathfrak{N}$ por la consistencia con A_E.

Teorema de Church (1936) El conjunto de los números de Gödel de los enunciados válidos (en el lenguaje de $\mathfrak{N}$) no es recursivo.

Demostración Se puede usar el teorema de indecidibilidad fuerte de $\mathrm{Cn}\, A_E$, tomando T como la mínima teoría del lenguaje, es decir, como el conjunto de los enunciados válidos. ⊣

El conjunto de números de Gödel de las fórmulas válidas tampoco es recursivo, pues, si lo fuera, entonces el conjunto de enunciados válidos también lo sería.

Esta prueba se aplica al lenguaje de $\mathfrak{N}$. Sin embargo, ni siquiera en un lenguaje con más parámetros el conjunto de enunciados válidos sería recursivo (pues, si lo fuera, entonces su intersección con el lenguaje $\mathfrak{N}$ sería recursiva). De hecho, es suficiente que el lenguaje tenga al menos un símbolo de predicado binario. (Véase el corolario 37G.) Por otro lado, es necesario establecer *algunas* cotas inferiores respecto del lenguaje para que se tenga indecidibilidad. Si el lenguaje tiene como único parámetro $\forall$ (lenguaje de la igualdad), entonces el conjunto de los enunciados válidos es decidible. (Véase el ejercicio 6.) También se sabe que si los únicos parámetros son $\forall$ y símbolos de predicado unarios, entonces el conjunto de fórmulas válidas es decidible.

Numerabilidad recursiva

Decimos que una relación es *recursivamente numerable* sii es de la forma

$$\{\vec{a} \mid \exists b\, \langle \vec{a}, b\rangle \in Q\}$$

con Q recursiva. Las relaciones recursivamente numerables desempeñan un papel muy importante dentro de la lógica, pues constituyen la contrapartida formal de las relaciones efectivamente numerables (como se explicará a continuación).

(La abreviatura canónica de "recursivamente numerable" es "r.n.";* cuando, en lugar de usar el término "recursivo", se usa

el término "calculable", entonces hablamos de relaciones *calculablemente numerables*, que se abrevia "c.n.")†

Las relaciones recursivamente numerables, al igual que las relaciones recursivas, son definibles en $\mathfrak{N}$. Si $\varphi(v_1, v_2)$ define en $\mathfrak{N}$ una relación binaria Q, entonces $\exists v_2 \varphi(v_1, v_2)$ define $\{a \mid \exists b \langle a,b\rangle \in Q\}$.

Teorema 35E Dada una relación m-aria R, las siguientes condiciones son equivalentes:

1. R es recursivamente numerable.
2. R es el dominio de una relación recursiva Q.
3. Existe una relación recursiva Q de $(m + 1)$ argumentos tal que

$$R = \{\langle a_1, \ldots, a_m\rangle \mid \exists b \langle a_1, \ldots, a_m, b\rangle \in Q\}.$$

4. Existe una relación recursiva Q de $(m + n)$ argumentos tal que

$$R = \{\langle a_1, \ldots, a_m\rangle \mid \exists b_1, \ldots, b_n \langle a_1, \ldots, a_m, b_1, \ldots, b_n\rangle \in Q\}.$$

Demostración 1 y 3 son equivalentes por definición. La equivalencia entre 2 y 3 se tiene por la definición de dominio y de $(m + 1)$-ada que dimos (en el capítulo cero). Por otro lado, está claro que 3 implica 4, así que lo único que tenemos que demostrar es que 4 implica 3. Esto es cierto porque

$$\begin{aligned} &\exists b_1, \ldots, b_n \langle a_1, \ldots, a_m, b_1, \ldots, b_n\rangle \in Q \\ &\text{sii} \exists c \langle a_1, \ldots, a_m, (c)_0, \ldots, (c)_{n-1}\rangle \in Q \end{aligned}$$

y

$$\{\langle a_1, \ldots, a_m, c\rangle \mid \langle a_1, \ldots, a_m, (c)_0, \ldots, (c)_{n-1}\rangle \in Q\}$$

es recursiva siempre que Q lo sea. (Nótese que hemos usado nuestra función decodificadora de sucesiones para colapsar una serie de cuantificadores en uno solo.) ⊣

*En inglés se abrevia "r.e.", de "recursively enumerable". [N. del t.]
†En inglés se abrevia "c.e.", por "computably enumerable". [N. del t.]

Por la parte 4 de este teorema, R es recursivamente numerable sii es definible en $\mathfrak{N}$ mediante una fórmula $\exists x_1 \cdots \exists x_n \varphi$, en la que φ está numeralmente determinada por A_E. De hecho, podemos pedir que φ sea una fórmula sin cuantificadores, resultado que se probó en 1961 (con exponenciación) y en 1970 (sin exponenciación). Las demostraciones involucran algunos resultados de la teoría de números, así que aquí las omitiremos.

Obsérvese que toda relación recursiva también es recursivamente numerable, ya que si R es recursiva, entonces está definida en $\mathfrak{N}$ por una fórmula $\exists x_1 \cdots \exists x_n \varphi$, donde φ es una fórmula numeralmente determinada por A_E y $x_1 \cdots x_n$ no ocurren en φ.

Teorema 35F Una relación es recursiva sii tanto ella como su complemento son recursivamente numerables.

Ésta es la contraparte formal del hecho (véase el teorema 17F) de que una relación es decidible sii tanto ella como su complemento son efectivamente numerables.

Demostración Si una relación es recursiva, entonces su complemento también lo es, de donde ambas son recursivamente numerables.

Por otro lado, supongamos que tanto P como su complemento son recursivamente numerables; entonces, para toda $\vec{a}$,

$$\vec{a} \in P \Leftrightarrow \exists b \, \langle \vec{a}, b \rangle \in Q$$
$$\vec{a} \notin P \Leftrightarrow \exists b \, \langle \vec{a}, b \rangle \in R$$

para algunas Q y R recursivas. Sea

$$f(\vec{a}) = \text{la mínima } b \text{ tal que o bien } \langle \vec{a}, b \rangle \in Q \text{ o bien } \langle \vec{a}, b \rangle \in R.$$

Siempre hay un número b que lo cumple y tenemos que f es recursiva. Por último,

$$\vec{a} \in P \Leftrightarrow \langle \vec{a}, f(\vec{a}) \rangle \in Q,$$

de modo que P es recursiva. ⊣

Las relaciones recursivamente numerables constituyen la contrapartida formal de las relaciones efectivamente numerables, como se puede ver con el siguiente resultado informal que se parece a la caracterización de la numerabilidad recursiva dada en el teorema 35E.

***Lema 35G** Una relación es efectivamente numerable sii es el dominio de una relación decidible.

Demostración Supongamos que Q se numera efectivamente mediante algún procedimiento. Entonces $\vec{a} \in Q$ sii $\exists n\,[\vec{a}$ aparece en la numeración en n pasos$]$. La relación definida entre corchetes es decidible y tiene como dominio a Q.

A la inversa, dada una relación decidible R, para enumerar $\{\langle a, b\rangle \mid \exists n\, \langle a, b, n\rangle \in R\}$ hay que revisar si $\langle (m)_0, (m)_1, (m)_2\rangle \in R$, para $m = 0, 1, 2, \ldots$ Cuando la respuesta sea afirmativa, habrá que colocar $\langle (m)_0, (m)_1\rangle$ en la lista de salida. ⊣

***Corolario 35H (Tesis de Church, segunda versión)** Una relación es efectivamente numerable sii es recursivamente numerable.

Demostración Al identificar la clase de las relaciones decidibles con la clase de las relaciones recursivas, estamos automáticamente identificando los dominios de las relaciones decidibles con los dominios de las relaciones recursivas. ⊣

De hecho, la segunda versión de la tesis de Church es equivalente a la primera. Para demostrar la primera versión a partir de la segunda, usamos los teoremas 35F y 17F.

Ya hemos demostrado, aunque usando otras palabras, que una teoría recursivamente axiomatizable es recursivamente numerable. No obstante, en este momento es importante replantearlo, pues nos muestra el papel que desempeña la numerabilidad recursiva dentro de la lógica.

Teorema 35I Si A es un conjunto de enunciados tal que $\sharp A$ es recursivo, entonces $\sharp\mathrm{Cn}\, A$ es recursivamente numerable.

Demostración Inciso 20 de la sección 4 de este capítulo. ⊣

En particular, $\sharp \mathrm{Cn} A_E$ es recursivamente numerable, aunque (por el teorema 35C) no es recursiva. En la próxima sección veremos otros ejemplos de conjuntos recursivamente numerables que no son recursivos.

Este teorema es la contraparte precisa del hecho intuitivo de que una teoría con un conjunto decidible de axiomas es efectivamente numerable (corolarios 25F y 26I). Nos muestra la diferencia entre lo que es *demostrable* en una teoría axiomática y lo que es *verdadero* en la estructura que se le asocia. Con un conjunto de axiomas recursivo, lo más que se puede tener es un conjunto de consecuencias recursivamente numerable; sin embargo, por el teorema de Tarski, $\mathrm{Th}\,\mathfrak{N}$ no es definible y mucho menos recursivamente numerable.

Aun si ampliamos nuestro lenguaje o añadimos nuevos axiomas, se sigue presentando el mismo fenómeno. Siempre que sea posible distinguir recursivamente lo que es una deducción de lo que no lo es, tendremos que el conjunto de teoremas es cuando mucho recursivamente numerable. Por ejemplo, el conjunto de enunciados de la teoría de números que son demostrables a partir de un sistema axiomático para la teoría de conjuntos es recursivamente numerable. Además, este conjunto incluye A_E y es consistente (a menos que nuestra elección del sistema axiomático haya sido muy extraña). De aquí se sigue que la teoría de conjuntos no es recursiva y es incompleta. (Esto último se discutirá con más detalle en la sección 7 de este capítulo.)

Representabilidad débil

Sea Q un conjunto recursivamente numerable, tal que

$$a \in Q \Leftrightarrow \exists b \, \langle a, b \rangle \in R$$

con R recursiva. Sabemos que existe una fórmula ρ que representa a R en $\mathrm{Cn}\, A_E$. Por lo tanto, la fórmula $\exists v_2 \rho$ define Q en $\mathfrak{N}$. Esta fórmula no puede representar a Q en $\mathrm{Cn}\, A_E$, a menos que Q sea recursiva. Sin embargo, puede hacerlo parcialmente.

$$
\begin{array}{lll}
a \in Q & \Rightarrow \langle a, b \rangle \in R & \text{para alguna } b \\
 & \Rightarrow A_E \vdash \rho(\mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0}) & \text{para alguna } b \\
 & \Rightarrow A_E \vdash \exists v_2\, \rho(\mathbf{S}^a\mathbf{0}, v_2) & \\
a \notin Q & \Rightarrow \langle a, b \rangle \notin R & \text{para toda } b \\
 & \Rightarrow A_E \vdash \neg\rho(\mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0}) & \text{para toda } b \\
 & \Rightarrow A_E \nvdash \exists v_2\, \rho(\mathbf{S}^a\mathbf{0}, v_2) &
\end{array}
$$

El último paso está justificado porque si $A_E \vdash \neg\varphi(\mathbf{S}^b\mathbf{0})$ para toda b, entonces $A_E \nvdash \exists x\, \varphi(x)$ (propiedad que se conoce con el nombre de *ω-consistencia*), pues es imposible que $\exists x\, \varphi(x), \neg\varphi(\mathbf{S}^0\mathbf{0}), \neg\varphi(\mathbf{S}^1\mathbf{0}), \ldots$ sean todas verdaderas en $\mathfrak{N}$.

Por lo tanto, tenemos que

$$a \in Q \Leftrightarrow A_E \vdash \exists v_2\, \rho(\mathbf{S}^a\mathbf{0}, v_2).$$

Parece conveniente dar una definición formal de esta mitad de la representabilidad.

Definición Sea Q una relación n-aria en $\mathbb{N}$, ψ una fórmula donde sólo $v_1, \ldots, v_n$ ocurren libres. Entonces ψ *representa débilmente* a Q en la teoría T sii para cualesquiera $a_1, \ldots, a_n$ en $\mathfrak{N}$,

$$\langle a_1, \ldots, a_n \rangle \in Q \Leftrightarrow \psi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_n}\mathbf{0}) \in T.$$

Obsérvese que si Q es representable en una teoría consistente T, entonces también es débilmente representable en T.

Teorema 35J Una relación es débilmente representable en $\mathrm{Cn}\, A_E$ sii es recursivamente numerable.

Demostración Acabamos de demostrar que una relación unaria recursivamente numerable Q es débilmente representable en $\mathrm{Cn}\, A_E$. En este caso se puede usar la misma prueba para Q n-aria, haciendo algunas modificaciones en la notación. A la inversa, si Q está débilmente representada por ψ en $\mathrm{Cn}\, A_E$, entonces

$$
\begin{aligned}
\langle a_1, \ldots, a_n \rangle \in Q \Leftrightarrow\ & \exists D\, [D \text{ es una deducción de } \psi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_n}\mathbf{0}) \text{ a partir de los axiomas } A_E] \\
\Leftrightarrow\ & \exists d\, \langle d, f(a_1, \ldots, a_n) \rangle \in P
\end{aligned}
$$

para alguna función recursiva f y una relación recursiva P. ⊣

Jerarquía aritmética

Decimos que una relación en los números naturales es *aritmética* sii es definible en $\mathfrak{N}$; sin embargo, algunas relaciones aritméticas son, en cierto sentido, más definibles que otras. Así que podemos establecer una jerarquía entre las relaciones aritméticas de acuerdo con su grado de definibilidad.

Sea Σ_1 la clase de las relaciones recursivamente numerables; estas relaciones "distan un cuantificador" de ser recursivas. Generalizando esta idea, definimos la clase de las relaciones Σ_k y la clase de las relaciones Π_k. Por ejemplo, las primeras clases están compuestas por relaciones de la forma que se presenta en la segunda columna:

Σ_1:	$\{\vec{a} \mid \exists b\, \langle \vec{a}, b \rangle \in R\}$,	R es recursiva.
Π_1:	$\{\vec{a} \mid \forall b\, \langle \vec{a}, b \rangle \in R\}$,	R es recursiva.
Σ_2:	$\{\vec{a} \mid \exists c\, \forall b\, \langle \vec{a}, b, c \rangle \in R\}$,	R es recursiva.
Π_2:	$\{\vec{a} \mid \forall c\, \exists b\, \langle \vec{a}, b, c \rangle \in R\}$,	R es recursiva.

En general, una relación Q pertenece a Π_k sii es de la forma

$$\{\vec{a} \mid \forall b_1\, \exists b_2 \cdots \Box b_k\, \langle \vec{a}, \vec{b} \rangle \in R\},$$

donde R es una relación recursiva. En este caso, "$\Box$" se sustituye por "$\forall$" si k es impar y por "$\exists$" si k es par. Análogamente, Q pertenece a Σ_k sii es de la forma

$$\{\vec{a} \mid \exists b_1\, \forall b_2 \cdots \Box b_k \langle \vec{a}, \vec{b} \rangle \in R\},$$

donde R es recursiva y "$\Box$" se sustituye por "$\exists$" si k es impar y por "$\forall$" si k es par.

Las clases Σ_k y Π_k también se pueden definir por recursión sobre k. Σ_1 es la clase de las relaciones recursivamente numerables. Lo siguiente es que una relación pertenece a Π_k sii su complemento está en Σ_k, y pertenece a Σ_{k+1} sii está en el dominio de una relación en Π_k. (Incluso se podría comenzar con $k = 0$, tomando Σ_0 como la clase de las relaciones recursivas.)

Ejemplo El conjunto de los números de Gödel de las fórmulas numeralmente determinadas por A_E está en Π_2.

Demostración a pertenece a este conjunto sii [a es el número de Gödel de una fórmula α] y $\forall b \exists d$[d es el valor de $\mathcal{G}$ asignado a una deducción, a partir de A_E, de $\alpha(\mathbf{S}^{(b)_0}0, \mathbf{S}^{(b)_1}0, \ldots)$ o de su negación]. Si recurrimos al método de la sección 4 de este capítulo, podemos demostrar que lo que se encuentra entre corchetes define relaciones recursivas y, utilizando la contraparte en español de la forma prenex, tenemos el conjunto descrito en la forma deseada:

$$\{a \mid \forall b \, \exists d \, \langle a, b, d, \rangle \in R\},$$

con R recursiva. ⊣

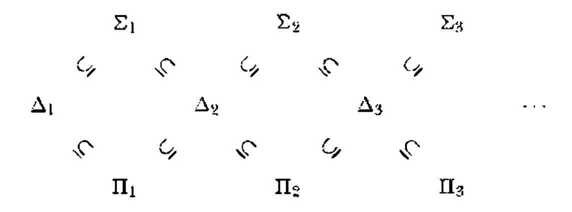
Una observación más sobre la notación: sea Δ_1 la clase de las relaciones recursivas. Entonces nuestro resultado previo (teorema 35F), que establece que una relación es recursiva sii tanto ella como su complemento son recursivamente numerables, puede expresarse ahora mediante la siguiente ecuación:

$$\Delta_1 = \Sigma_1 \cap \Pi_1.$$

Como esta ecuación se cumple, definimos Δ_n para $n > 1$ mediante la ecuación análoga,

$$\Delta_n = \Sigma_n \cap \Pi_n.$$

Las siguientes inclusiones se cumplen:



El caso $\Delta_1 \subseteq \Sigma_1$ ya se había mencionado antes (véase el teorema 35F); su demostración se basaba en la posibilidad de la

"cuantificación vacía". Las demostraciones de los otros casos son conceptualmente las mismas. Si x no ocurre en φ, entonces φ, $\forall x\ \varphi$, $\exists x\ \varphi$ son todas equivalentes. Por ejemplo, una relación en Σ_1 está definida por una fórmula del tipo $\exists y\ \varphi$, con φ numeralmente determinada por A_E. Pero la misma relación está definida por $\exists y \forall x\ \varphi$ y $\forall x \exists y\ \varphi$ (donde x no ocurre en φ). Por lo tanto, la relación también está en Σ_2 y Π_2.

También es cierto que todas estas inclusiones son propias, es decir, que la igualdad no se cumple; sin embargo, esto no lo probaremos aquí. En la figura 10 se muestra un diagrama de las inclusiones.

La clase de las relaciones aritméticas es igual a $\bigcup_k \Sigma_k$, aunque también a $\bigcup_k \Pi_k$. Por ejemplo, toda relación en Σ_2 es aritmética, pues está definida en $\mathfrak{N}$ por una fórmula del tipo $\exists x \forall y\ \varphi$, con φ numeralmente determinada por A_E. A la inversa, toda relación aritmética está definida en $\mathfrak{N}$ por una fórmula prenex. La parte sin cuantificadores de esa fórmula prenex define una relación recursiva (ya que las fórmulas sin cuantificadores están numeralmente determinadas por A_E). Por lo tanto, la relación definida se ubica en algún lugar de la jerarquía. El método de "colapsar" los cuantificadores $\exists\exists \cdots \exists$ que se usa en la demostración del teorema 35E (y el método dual aplicado a $\forall\forall \cdots \forall$) puede ser de gran utilidad aquí.

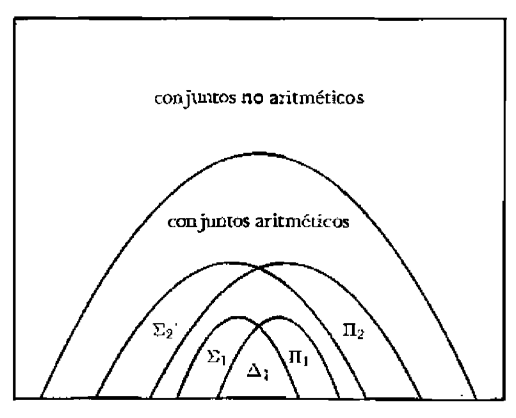


FIGURA 10. *Diagrama de* $\mathcal{PN}$

Tenemos un resultado que relaciona la definibilidad en $\mathfrak{N}$ con la jerarquía que construimos a partir de las relaciones recursivas:

Teorema 35K Una relación sobre los números naturales es aritmética (es decir, definible en $\mathfrak{N}$) sii pertenece a Σ_k para alguna k, y esta propiedad, a su vez, es equivalente a pertenecer a Π_l para alguna l.

En particular, toda relación recursivamente numerable es aritmética, como ya se había señalado antes.

Hay algunos trucos que sirven para localizar relaciones aritméticas específicas dentro de esta jerarquía. Por ejemplo, sea A el conjunto de números de Gödel de fórmulas α, tales que para alguna n,

$$A_E \vdash \alpha(\mathbf{S}^n\mathbf{0}) \quad \text{y} \quad (\forall i < n)\ A_E \vdash \neg\alpha(\mathbf{S}^i\mathbf{0}).$$

Entonces $a \in A$ sii [a es el número de Gödel de una fórmula α] y $\exists n\ \exists D$[D es una deducción de $\alpha(\mathbf{S}^n\mathbf{0})$ a partir de A_E] y $(\forall i < n)\ (\exists D_i)$[$D_i$ es una deducción de $\neg\alpha(\mathbf{S}^i\mathbf{0})$ a partir de A_E]. Las partes entre corchetes son recursivas, de modo que sólo hay que considerar los cuantificadores que quedan fuera. El cuantificador acotado "$\forall i < n$" no cuenta, pues tenemos que

$$(\forall i < n)(\exists d)\langle d,i\rangle \in P \Leftrightarrow (\exists d)(\forall i < n)\langle (d)_i, i\rangle \in P.$$

Basándonos en este hecho, podemos integrar el cuantificador acotado a la parte recursiva y, por lo tanto, $A \in \Sigma_1$.

El siguiente teorema generaliza el teorema 35I.

Teorema 35L Sea A un conjunto de enunciados tal que $\sharp A$ pertenece a Σ_k, con $k > 0$. Entonces, $\sharp\text{Cn}\, A$ también pertenece a Σ_k.

Demostración Recordemos las demostraciones de los incisos 18 y 20 de la sección 4 de este capítulo. Ahí teníamos que

$a \in \sharp\text{Cn}\, A \leftrightarrow a$ es el número de Gödel de un enunciado y $\exists d[d$ es un número de sucesión y el último componente de d es a y para toda i menor que $\text{lh}d$, o bien (1) $(d)_i \in \sharp A$, (2) $(d)_i$ es el número de Gödel de un axioma lógico, o (3) para algunas j y l menores que i, $(d)_j = \langle h(()\rangle * (d)_l * \langle h(\rightarrow)\rangle * (d)_i * \langle h())\rangle]$.

Dado que $\sharp A \in \Sigma_k$, en (1) debemos reemplazar "$(d)_i \in \sharp A$" por algo de la forma

$$\exists b_1 \forall b_2 \cdots \Box b_k \; \langle (d)_i, \vec{b}\rangle \in Q$$

con Q recursiva. Faltaría transformar esto en una expresión prenex en español de la forma Σ_k. Sugerimos que el lector trate de hacerlo para el caso $k = 2$, y que ponga el procedimiento por escrito. El artificio del ejemplo anterior será de utilidad. ⊣

Ejercicios

1. Muestre que no existe un conjunto recursivo R tal que $\sharp\text{Cn}A_E \subseteq R$ y $\sharp\{\sigma \mid (\neg\sigma) \in \text{Cn}A_E\} \subseteq \overline{R}$, el complemento de R. (Este resultado puede reformularse de la siguiente manera: los teoremas de A_E no se pueden separar recursivamente de los enunciados refutables.) *Sugerencia*: Construya un enunciado σ que diga "mi número de Gödel *no* está en R" y trate de ver dónde está $\sharp\sigma$.

2. Sea A un conjunto recursivo de enunciados dentro de un lenguaje recursivamente numerado con $\mathbf{0}$ y S. Suponga que toda relación recursiva es representable en la teoría Cn A. Suponga incluso que A es ω-consistente; es decir, que no existe una fórmula φ tal que $A \vdash \exists x\, \varphi(x)$ y para toda $a \in \mathbb{N}$, $A \vdash \neg\varphi(\text{S}^a\mathbf{0})$. Construya un enunciado σ que indirectamente diga que no es un teorema de A y muestre que ni $A \vdash \sigma$ ni $A \vdash \neg\sigma$. *Sugerencia*: Revise la sección cero del capítulo III.

   Observación: Ésta es una versión del teorema de incompletud más cercana al argumento original de Gödel de 1931. Obsérvese que no se pide que los axiomas de A

sean *verdaderos* en $\mathfrak{N}$. Tampoco se pide que A contenga a A_E; no obstante, se puede usar el argumento del punto fijo.

3. Sea T una teoría en un lenguaje recursivamente numerado (con $\mathbf{0}$ y $\mathbf{S}$). Suponga que todos los subconjuntos recursivos de $\mathbb{N}$ son débilmente representables en T. Muestre que $\sharp T$ no es recursivo. *Sugerencia:* Construya una relación binaria P tal que todo subconjunto de $\mathbb{N}$ débilmente representable sea igual a $\{b \mid \langle a, b\rangle \in P\}$ para alguna a, y tal que P sea recursivo si $\sharp T$ lo es. Considere el conjunto $H = \{b \mid \langle b, b\rangle \notin P\}$. Vea la sección cero del capítulo III. Se puede adaptar aquí lo que allá se dijo del "argumento diagonal" para el caso especial de $T = \text{Th}\,\mathfrak{N}$.
   Observación: Este ejercicio ofrece otra versión del resultado "cualquier teoría suficientemente fuerte es indecidible".

4. Muestre que hay $2^{\aleph_0}$ modelos numerables, no isomorfos, de $\text{Th}\,\mathfrak{N}$. *Sugerencia:* Para cada conjunto A de números primos, encuentre un modelo que tenga un elemento divisible exactamente entre los primos de A.

5. (Lindenbaum) Sea T una teoría decidible y consistente (en un lenguaje razonable). Muestre que T puede extenderse a una teoría completa, decidible y consistente T'. *Sugerencia:* Revise uno a uno cada enunciado σ y añada o bien σ, o bien $\neg\sigma$ a T, pero asegúrese de preservar la decidibilidad.

6. Considere el lenguaje de la igualdad, que tiene a $\forall$ como único parámetro. Sea λ_n la traducción de "Hay al menos n cosas"; vea la demostración del teorema 26A. Diremos que una fórmula es *simple* sii puede construirse a partir de fórmulas atómicas y las fórmulas λ_n usando conectivos (pero no cuantificadores). Muestre que, dada cualquier fórmula en el lenguaje de la igualdad, se puede encontrar una fórmula simple que sea lógicamente equivalente a ella. *Sugerencia:* Vea esto como un resultado del tipo de los de eliminación de cuantificadores (donde los cuantificadores de λ_n no cuentan). Use el teorema 31F.

7. (a) Suponga que A y B son subconjuntos de $\mathbb{N}$ que pertenecen a Σ_k (o a Π_k). Muestre que $A \cup B$ y $A \cap B$ también pertenecen a Σ_k (o a Π_k, respectivamente).

   (b) Suponga que A pertenece a Σ_k (o a Π_k) y que las funciones $f_1, \ldots, f_m$ son recursivas. Muestre que

$$\{\vec{a} : \langle f_1(\vec{a}), \ldots, f_m(\vec{a})\rangle \in A\}$$

   también pertenece a Σ_k (o a Π_k, respectivamente). *Sugerencia*: Comience por demostrarlo para Σ_1 y observe que el argumento que se usa para ese caso se puede generalizar.

8. Sea T una teoría en un lenguaje recursivamente numerado (con $\mathbf{0}$ y $\mathbf{S}$). Sea n fija, $n \geq 0$. Suponga que todos los subconjuntos de $\mathbb{N}$ en Σ_n son débilmente representables en T. Muestre que $\sharp T$ no pertenece a Π_n. (Observe que el ejercicio 3 es un caso especial de esto, con $n = 0$. Las sugerencias que se dan ahí también sirven para este ejercicio.)

9. Muestre que el conjunto

$$\{\sharp\sigma \mid A_E; \sigma \text{ es } \omega\text{-consistente}\}$$

   (véase el ejercicio 2) pertenece a Π_3.

10. La teoría $\mathrm{Cn}\, A_E$ tiene muchas extensiones completas, de las cuales $\mathrm{Th}\,\mathfrak{N}$ es sólo una. Pero, ¿cuántas hay?; es decir, ¿cuál es la cardinalidad del conjunto de teorías completas (en el lenguaje) que extienden A_E?

6. *Funciones recursivas*

Hemos utilizado funciones recursivas (es decir, funciones que, consideradas como relaciones, son recursivas) para obtener los teoremas de incompletud e indecidibilidad de teorías. Sin embargo, la clase de las funciones recursivas es en sí misma muy interesante, así que a lo largo de esta sección revisaremos algunas de sus propiedades.

Recuérdese que, por la tesis de Church, una función es recursiva sii es calculable mediante un procedimiento efectivo (véase el comentario posterior al teorema 33H). Este resultado es, en realidad, el que hace que las funciones recursivas sean atractivas; asimismo, nos permite entender intuitivamente la recursividad, lo que facilita mucho su estudio. Supongamos, por ejemplo, que alguien nos pregunta si la inversa de una permutación recursiva en $\mathbb{N}$ es recursiva. Antes de intentar demostrarlo, tendríamos que plantearnos la pregunta en términos más intuitivos: ¿es calculable la inversa de una permutación calculable f? Entonces parece más fácil de ver —o al menos eso esperamos— que la respuesta es afirmativa. Para calcular $f^{-1}(3)$, se pueden calcular $f(0), f(1), \ldots$ hasta que se encuentre una k tal que $f(k) = 3$. Entonces $f^{-1}(3) = k$. Este procedimiento tiene dos grandes ventajas. Por un lado, nos da la certeza de que la respuesta a la pregunta sobre las permutaciones recursivas también es afirmativa. Por el otro, nos da una buena idea de cómo demostrarlo, pues sólo necesitamos formalizar esta prueba intuitiva. Esta estrategia para abordar los problemas conectados con la recursividad será de gran utilidad a lo largo de esta sección.

Antes de continuar, tal vez valga la pena hacer un recuento de algunos de los resultados que hemos obtenido sobre las funciones recursivas. Sabemos, por el teorema 34A, que una función f es recursiva sii es representable (como relación) en Cn A_E. Por lo tanto, toda función recursiva es débilmente representable en esta teoría.

En la sección 3 de este capítulo se dio un repertorio de funciones recursivas. Además se mostró que la clase de las funciones recursivas es cerrada bajo ciertas operaciones, como la composición (teorema 33L) y el operador "mínimo cero" (teorema 33M).

Sabemos también que hay algunas funciones que no son recursivas. De hecho, hay una cantidad no numerable ($2^{\aleph_0}$ para ser precisos) de funciones de $\mathbb{N}^m$ en $\mathbb{N}$, de las cuales sólo una cantidad numerable pueden ser recursivas. Así que tenemos una gran cantidad de funciones no recursivas, a pesar de que en la sección 3 de este capítulo se mostró que las funciones más comunes (como los polinomios) son recursivas. Por el in-

ciso 1 del catálogo de dicha sección 3, tenemos que la función característica de un conjunto no recursivo es no recursiva. Por ejemplo, si $f(a) = 1$ cuando a es el número de Gódel de un elemento de $\mathrm{Cn}\, A_E$ y $f(a) = 0$ en caso contrario, entonces f no es recursiva.

Forma normal

Para toda función calculable, como es el caso de la función polinomial $a^2 + 3a + 5$, es posible, al menos en principio, diseñar una computadora digital que, tras introducir a, nos dé como salida $a^2 + 3a + 5$ (Fig. 11). Sin embargo, si queremos trabajar con otra función, es necesario construir una computadora distinta (o rehacer las conexiones de la que se tiene). Desde hace tiempo se tiene claro que, en la mayoría de los casos, lo ideal es construir una sola computadora para funciones generales, que permita guardar programas, en cuyo caso no sólo es necesario dar a, sino también el programa para calcular el polinomio (Fig. 12). Esta computadora "universal" necesita dos entradas, y siempre que se introduzca el programa adecuado, puede calcular cualquier función unaria calculable (suponiendo que se tiene suficiente espacio para memoria). Desde luego que hay programas que no generan ninguna función sobre $\mathbb{N}$, como bien lo sabe y resiente cualquier programador de computadoras. (¡Lo que sí producen esos programas son crisis!)

En lo que queda de esta subsección y la siguiente, repetiremos lo que acabamos de decir, pero para funciones recursivas y con demostraciones. Para nuestra computadora universal tendremos una relación recursiva T_1 y una función recursiva U. Entonces, dada cualquier función recursiva $f: \mathbb{N} \to \mathbb{N}$, existirá una e (análoga al programa) tal que

$$\begin{aligned} f(a) &= U(\text{la mínima } k \text{ tal que } \langle e, a, k\rangle \in T_1) \\ &= U(\mu k\, \langle e, a, k\rangle \in T_1), \end{aligned}$$

donde la segunda ecuación debe entenderse como una abreviación de la primera. De hecho, e será el número de Gödel de una fórmula φ que representa a f (al menos débilmente) en $\mathrm{Cn}A_E$. Y los números k tales que $\langle e, a, k\rangle \in T_1$ codificarán

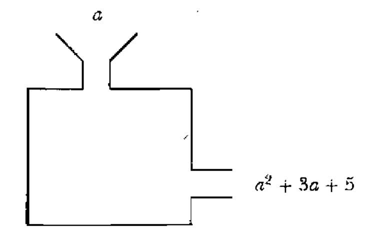


FIGURA 11. *Computadora para una función especial*

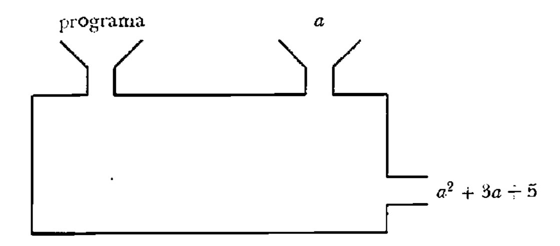


FIGURA 12. *Computadora para funciones generales*

tanto $f(a)$ como $\mathcal{G}$ de una deducción de $\varphi(\mathbf{S}^a\mathbf{0}, \mathbf{S}^{f(a)}\mathbf{0})$ a partir de A_E.

Definición Para todo número entero positivo m, T_m será la relación de $(m + 2)$ argumentos a la que pertenece la $(m + 2)$-ada $\langle e, a_1, \ldots, a_m, k\rangle$ sii

(i) e es el número de Gödel de una fórmula φ en la cual sólo $v_1, \ldots, v_m, v_{m+1}$ ocurren libres;

(ii) k es un número de sucesión de longitud 2 y $(k)_0$ es $\mathcal{G}$ de una deducción, a partir de A_E, de $\varphi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}, \mathbf{S}^{(k)_1}\mathbf{0})$.

La idea aquí es que, para toda función recursiva f, antes que cualquier otra cosa, lo que hay que hacer es tomar e como el número de Gödel de una fórmula φ que represente débilmente f

(como relación). Entonces sabemos que para cualesquiera a y b,

$$A_E \vdash \varphi(\mathbf{S}^a\mathbf{0},\mathbf{S}^b\mathbf{0}) \quad \text{sii} \quad b = f(a).$$

De modo que cualquier número k que cumpla con el inciso (ii) de la definición debe ser igual a $\langle (k)_0, f(a)\rangle$, donde $(k)_0$ es $\mathcal{G}$ de una deducción de $\varphi(\mathbf{S}^a\mathbf{0}, \mathbf{S}^{f(a)}\mathbf{0})$ a partir de A_E. (En este caso, nos estamos alejando de la definición más común de T_m, al no pedir que k sea la más pequeña posible.)

Tómese como función "conclusiva" U la función

$$U(k) = (k)_1.$$

La U definida de este modo es recursiva y, por lo establecido en el párrafo anterior, tenemos que $U(k) = f(a)$.

Lema 36A Para toda m, la relación T_m es recursiva.

Demostración para $m = 2$ $\langle e, a_1, a_2, k\rangle \in T_2$ sii e es el número de Gödel de una fórmula, $\sharp(\forall v_1, \forall v_2, \forall v_3) * e$ es el número de Gödel de un enunciado, k es un número de sucesión de longitud 2 y $(k)_0$ es $\mathcal{G}$ de una deducción, a partir de A_E, de

$$\text{Sb}\,(\text{Sb}\,(\text{Sb}\,(e, \sharp v_1, g\,(a_1)), \sharp v_2, g\,(a_2)), \sharp v_3, g\,((k)_1)),$$

con $g(n) = \sharp\mathbf{S}^n\mathbf{0}$. Gracias a la sección 4 de este capítulo sabemos que todo esto es recursivo. ⊣

Teorema 36B (a) Para toda función recursiva $f : \mathbb{N}^m \to \mathbb{N}$, existe una e tal que para cualesquiera $a_1, \ldots, a_m$,

$$f(a_1, \ldots, a_m) = U(\mu k\ \langle e, a_1, \ldots, a_m, k\rangle \in T_m).$$

(En particular, dicho número k existe.)

(b) A la inversa, para cualquier e, tal que $\forall a_1, \cdots, a_m\ \exists k\ \langle e, a_1, \ldots, a_m, k\rangle \in T_m$, la función cuyo valor en $a_1, \ldots, a_m$ es $U(\mu k\ \langle e, a_1, \ldots, a_m, k\rangle \in T_m)$ es recursiva.

Demostración El inciso (b) se sigue inmediatamente del hecho de que U y T_m son recursivas. Para el caso del inciso (a) tomamos e como el número de Gödel de una fórmula φ que representa débilmente a f en Cn A_E. Dada cualquier $\vec{a}$, sabemos que $A_E \vdash \varphi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}, \mathbf{S}^{f(\vec{a})}\mathbf{0})$. Sea

d el valor de $\mathcal{G}$ de una deducción de este enunciado a partir de A_E, entonces $\langle e, \vec{a}, \langle d, f(\vec{a})\rangle\rangle \in T_m$. Así que hay un número k tal que $\langle e, \vec{a}, k\rangle \in T_m$. Para toda k que cumpla eso, sabemos que $A_E \vdash \varphi(S^{a_1}0, \ldots, S^{a_m}0, S^{(k)_1}0)$, pues $(k)_0$ es $\mathcal{G}$ de una deducción; en consecuencia, por nuestra elección de $\varphi, U(k) = (k)_1 = f(\vec{a})$. Entonces tenemos que $U(\mu k\ \langle e, \vec{a}, k\rangle \in T_m) = f(\vec{a})$. ⊣

Este teorema, formulado por Kleene en 1936, nos muestra que toda función recursiva es representable en la forma normal

$$f(\vec{a}) = U(\mu k\ \langle e, \vec{a}, k\rangle \in T_m).$$

Tenemos, entonces, que una computadora que sea capaz de calcular U y la función característica de T_1 es una computadora "universal" para las funciones recursivas de un argumento. La entrada e corresponde al programa y debe elegirse con cuidado si se quiere que arroje resultados (es decir, si es que hay una k tal que $\langle e, a, k\rangle \in T_1$).

Funciones parciales recursivas

La teoría sobre las funciones recursivas es más significativa si la consideramos dentro del contexto más general de las funciones parciales.

Definición Una *función parcial* de m argumentos es una función f tal que $\operatorname{dom} f \subseteq \mathbb{N}^m$ y $\operatorname{ran} f \subseteq \mathbb{N}$. Si $\vec{a} \notin \operatorname{dom} f$, entonces se dice que $f(\vec{a})$ *es indefinida*. Si $\operatorname{dom} f = \mathbb{N}^m$, se dice que f es *total*.

El lector no debe tomar de manera demasiado literal las palabras "parcial" y "total" (como tampoco el término "indefinida"), pues no se trata de casos mutuamente excluyentes. Una función parcial f puede ser total o no. Por lo que, en nuestro caso, los términos "total" y "parcial" no deben ser vistos como antónimos.

Comenzaremos por estudiar las funciones parciales que son intuitivamente calculables.

*Definición Una función parcial f de m argumentos es *calculabe* sii existe un procedimiento efectivo tal que (a) dada

una m-ada $\vec{a}$ en dom f, el procedimiento nos da $f(\vec{a})$; y (b) dada una m-ada $\vec{a}$ que no pertenece a dom f, el procedimiento no da resultado alguno.

Esta definición extiende a las funciones parciales la definición de función calculable que habíamos dado para las funciones totales. En ese entonces demostramos un resultado (teorema 33H), parte del cual podría extenderse a las funciones parciales.

***Teorema 36C** Una función parcial de m argumentos es calculable sii f (vista como una relación de $(m + 1)$ argumentos) es efectivamente numerable.

Demostración Esta demostración hace eco de la demostración de otro resultado, el teorema 17E. Primero supongamos que tenemos una forma efectiva de numerar f. Dada una m-ada $\vec{a}$, revisamos la lista de los elementos de la relación que se va formando conforme se aplica el procedimiento. Cuando aparezca, si es que lo hace, una $(m + 1)$-ada que comience con $\vec{a}$, tomamos su última componente como $f(\vec{a})$.

A la inversa, sea f una función calculable. Supongamos primero que f es una función parcial de un argumento. Podemos numerar f como relación, mediante el siguiente procedimiento:

1. Tomar un minuto para calcular $f(0)$.

2. Tomar dos minutos para calcular $f(0)$ y después otros dos minutos para calcular $f(1)$.

3. Tomar tres minutos para calcular $f(0)$, otros tres para calcular $f(1)$ y otros tres para calcular $f(2)$.

Y así sucesivamente. Desde luego que en el momento en que alguno de estos cálculos se concluya, debe escribirse el par correspondiente en la lista de elementos de la relación f.

Para el caso en que f sea una función parcial calculable de m argumentos, en lugar de calcular los valores de f en 0, 1, 2, ..., calculamos sus valores en $((0)_0, \cdots,$

$(0)_{m-1}\rangle$, $\langle(1)_0, \ldots, (1)_{m-1}\rangle$, $\langle(2)_0, \ldots, (2)_{m-1}\rangle$, etcétera. ⊣

En el caso de las funciones totales calculables también habíamos concluido que f era una relación decidible; sin embargo, esto puede fallar para algunas funciones f no totales. Por ejemplo, sea

$$f(a) = \begin{cases} 0 & \text{si } a \in \sharp\mathrm{Cn}\, A_E, \\ \text{indefinida} & \text{en otro caso.} \end{cases}$$

En este caso, f es calculable. (Se puede obtener $f(a)$ listando los elementos de $\sharp\mathrm{Cn}\, A_E$ y buscando a.) Sin embargo, f no es una relación decidible, pues de otro modo $\sharp\mathrm{Cn}\, A_E$ sería decidible. Este ejemplo y el siguiente teorema explican nuestra decisión de dar una definición de lo que sería exactamente la contraparte formal del concepto de función parcial calculable.

Definición Una *función parcial recursiva* es una función parcial tal que, vista como relación, es recursivamente numerable.

Debemos advertir al lector que la frase "función parcial recursiva" es indivisible; una función parcial recursiva (vista como relación) *no* necesariamente es recursiva. Pero al menos esta terminología es consistente con la forma en que nos hemos expresado hasta ahora para el caso de las funciones totales.

Teorema 36D Sea $f : \mathbb{N}^m \to \mathbb{N}$ una función total. Entonces f es una función parcial recursiva sii f es recursiva (como relación).

Demostración Si f es recursiva (como relación), entonces f es *a fortiori* recursivamente numerable. A la inversa, supongamos que f es recursivamente numerable. Como f es total,

$$f(\vec{a}) \neq b \iff \exists c\, [f(\vec{a}) = c \text{ y } b \neq c].$$

La expresión del lado derecho muestra que el complemento de f también es recursivamente numerable. De manera que, por el teorema 35F, f es recursiva. ⊣

Cuando comenzamos a discutir algunos de los resultados de la forma normal, nos tratamos de imaginar un aparato con

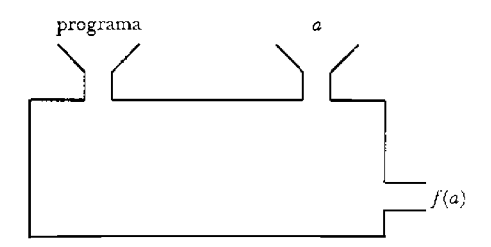


FIGURA 13. *Computadora con un programa para* f.

dos entradas (Fig. 13). Vimos que, para toda función parcial calculable, existe un programa que la calcula. Pero ahora también tenemos que el inverso es cierto: todo programa produce una función *parcial* calculable. Desde luego, muchos programas generan la función vacía, pero ésa es una función parcial calculable.

Estas consideraciones pueden aplicarse también al caso de las funciones parciales recursivas. Defínase como sigue la función parcial de m argumentos $[[e]]_m$ para cada $e \in \mathbb{N}$

$$[[e]]_m(a_1, \ldots, a_m) = U(\mu k\ \langle e, a_1, \ldots, a_m, k\rangle \in T_m).$$

En caso de que dicha k no exista, el lado derecho debe entenderse como indefinido. En otras palabras,

$$\vec{a} \in \operatorname{dom}[[e]]_m \quad \text{sii} \quad \exists k\ \langle e, a_1, \ldots, a_m, k\rangle \in T_m,$$

en cuyo caso el valor de $[[e]]_m(\vec{a})$ está dado por la ecuación previa.

El siguiente teorema es una versión mejorada del teorema 36B:

Teorema de la forma normal (Kleene, 1943) (a) La función parcial de $(m + 1)$ argumentos cuyo valor en $\langle e, a_1, \ldots, a_m\rangle$ es $[[e]]_m(a_1, \ldots, a_m)$ es una función parcial recursiva.

(b) Para toda $e \geq 0$, $[[e]]_m$ es una función parcial recursiva de m argumentos.

(c) Toda función parcial recursiva de m argumentos es igual a $[[e]]_m$, para alguna e.

Demostración (a) Tenemos que

$$[[e]]_m(\vec{a}) = b \Leftrightarrow \exists k [\langle e, \vec{a}, k\rangle \in T_m \text{ y } U(k) = b \text{ y } (\forall k' < k)\langle e, \vec{a}, k'\rangle \notin T_m].$$

La parte entre corchetes es recursiva, así que la función (vista como relación) es recursivamente numerable.

(b) Aunque en este caso e está fija, la demostración anterior sirve.

(c) Sea f una función parcial recursiva de m argumentos, tal que $\{\langle \vec{a}, b\rangle \mid f(\vec{a}) = b\}$ es recursivamente numerable. Por lo tanto, existe una fórmula φ que representa débilmente a esta relación en Cn A_E. Afirmamos que $f = [[\sharp\varphi]]_m$, pues si $f(\vec{a}) = b$, entonces $A_E \vdash \varphi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}, \mathbf{S}^{b}\mathbf{0})$. Por lo tanto, existe una k tal que $\langle \sharp\varphi, \vec{a}, k\rangle \in T_m$. Por otro lado, para toda k que cumple eso, $U(k) = b$, pues $A_E \nvdash \varphi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}, \mathbf{S}^{c}\mathbf{0})$ para toda $c \neq b$. De manera similar, si $f(\vec{a})$ está indefinida, entonces $A_E \nvdash \varphi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}, \mathbf{S}^{c}\mathbf{0})$ para toda c, y entonces también $[[\sharp\varphi]]_m$ está indefinida. ⊣

La parte (a) del teorema de la forma normal nos dice (en el caso en que $m = 1$) que la función Φ dada por la ecuación

$$\Phi(e,a) = [[e]]_1(a) = U(\mu k\ \langle e, a, k\rangle \in T_1)$$

es una función parcial recursiva. La parte (c) nos dice que Φ es "universal" en el sentido de que podemos obtener cualquier función parcial recursiva de un argumento si damos un valor fijo y adecuado a la primera variable de Φ.

La contraparte intuitiva de la función universal Φ es el sistema operativo de una computadora. El sistema operativo tiene dos entradas, el programa e y la información a, y deja correr el programa con dicha información. Pero el sistema operativo es en sí mismo *calculable*, si se ve como una función parcial de dos argumentos.

La demostración del teorema de la forma normal nos da un procedimiento para calcular los valores de nuestro "sistema

operativo" Φ, aunque de una manera extremadamente ineficiente. La idea sencilla de "examinar el programa e y dejarlo correr con la información a" se complica bastante, por decir lo menos.

Decimos que la función $[\![e]\!]_m$ es la función parcial recursiva de m argumentos con *índice e*. La parte (c) del teorema de la forma normal nos dice que toda función parcial recursiva tiene un índice. La demostración nos muestra que el número de Gödel de una fórmula que representa débilmente a una función siempre es un índice de dicha función.

Tenemos, entonces, una lista indexada $[\![0]\!]_1 [\![1]\!]_1, \ldots$ de las funciones parciales recursivas de un argumento. La función $[\![e]\!]_1$ se genera a partir de las "instrucciones" codificadas por e. Desde luego, la función será vacía, a menos que e sea el número de Gödel de una fórmula y se cumplan otras condiciones particulares.

Todas las funciones totales recursivas están dentro de nuestra lista de funciones parciales recursivas. Sin embargo, dado un número e, no tenemos una forma efectiva de decidir si es o no el índice de alguna función total:

Teorema 36E $\{e \mid [\![e]\!]_1 \text{ es total}\}$ no es recursivo.

Demostración Llámese a este conjunto A. Considérese la función definida por

$$f(a) = \begin{cases} [\![a]\!]_1(a) + 1 & \text{si } a \in A, \\ 0 & \text{si } a \notin A. \end{cases}$$

Entonces, por construcción, f es total. ¿Será recursiva? Tenemos que

$$f(a) = b \iff [(a \notin A \text{ y } b = 0) \text{ o } (a \in A \text{ y } \exists k[\langle a, a, k\rangle \in T_1 \\ \text{y } b = U(k) + 1 \text{ y } (\forall j < k)\langle a, a, j\rangle \notin T_1))].$$

Por lo tanto, si A es recursivo, entonces f es recursivamente numerable (como relación). Pero entonces f es una función total recursiva, así que es igual a $[\![e]\!]_1$ para alguna $e \in A$. Ahora bien, $f(e) = [\![e]\!]_1(e) + 1$, de modo que no es posible que $f = [\![e]\!]_1$. Esta contradicción demuestra que A no puede ser recursivo. ⊣

No es difícil mostrar que A está en Π_2. Ésta es la mejor clasificación que podemos hacer de A, pues se puede probar que A no pertenece a Σ_2.

Teorema 36F El conjunto

$$K = \{a \mid [[a]]_1(a) \text{ está definida}\}$$

es recursivamente numerable, pero no es recursivo.

Demostración K es recursivamente numerable, ya que $a \in K \Leftrightarrow \exists k \langle a, a, k \rangle \in T_1$. Para ver que K no es recursivo, considere la función dada por:

$$g(a) = \begin{cases} [[a]]_1(a) + 1 & \text{si } a \in K, \\ 0 & \text{si } a \notin K. \end{cases}$$

Ésta es una función total. Exactamente igual que para el teorema anterior, tenemos que K no puede ser recursivo. ⊣

Corolario 36G (La insolubilidad del problema de la detención) La relación

$$\{\langle e, a \rangle \mid [[e]]_1(a) \text{ está definida}\}$$

no es recursiva.

Demostración Tenemos que $a \in K$ sii $\langle a, a \rangle$ pertenece a esta relación. (De modo que el problema de la pertenencia a K es "reducible" al problema de la detención.) Si esta relación fuera recursiva, entonces K sería recursivo, pero no lo es. ⊣

Este corolario nos dice que, dado un programa e para una función parcial recursiva y una *entrada* a, no hay forma efectiva de decidir si la función $[[e]]_1$ está definida o no en a.

Es posible indexar las relaciones recursivamente numerables si hacemos uso de la siguiente caracterización:

Teorema 36H Una relación sobre $\mathbb{N}$ es recursivamente numerable sii es el dominio de una función parcial recursiva.

Demostración El dominio de toda función recursivamente numerable también es recursivamente numerable (véase la

parte 4 del teorema 35E). En particular, el dominio de toda función parcial recursiva es recursivamente numerable.

A la inversa, sea Q una relación recursivamente numerable tal que

$$\vec{a} \in Q \Leftrightarrow \exists b \, \langle \vec{a}, b \rangle \in R$$

con R recursiva. Sea

$$f(\vec{a}) = \mu b \, \langle \vec{a}, b \rangle \in R;$$

es decir,

$$f(\vec{a}) = b \Longleftrightarrow \langle \vec{a}, b \rangle \in R \text{ y } (\forall c < b) \, \langle \vec{a}, c \rangle \notin R.$$

Entonces f, como relación, es recursiva. Por lo tanto, f es una función parcial recursiva que claramente tiene como dominio a Q. ⊣

Vemos, entonces, que nuestra indexación sobre las funciones parciales recursivas induce una indexación sobre las relaciones recursivamente numerables. Sea

$$W_e = \operatorname{dom} [\![e]\!]_1.$$

Entonces $W_0, W_1, W_2, \ldots$ es una lista de todos los subconjuntos recursivamente numerables de $\mathbb{N}$. En el teorema 36E mostramos que $\{e \mid W_e = \mathbb{N}\}$ no es recursivo. El teorema 36F nos asegura que $\{e \mid e \in W_e\}$ tampoco es recursivo. Definamos la relación Q de la siguiente manera:

$$Q = \{\langle e, a \rangle \mid a \in W_e\}.$$

Como $\langle e, a \rangle \in Q \Leftrightarrow \exists k \langle e, a, k \rangle \in T_1$, entonces Q es recursivamente numerable. Más aún, Q es universal para los conjuntos recursivamente numerables, lo que quiere decir que, para todo conjunto recursivamente numerable $A \subseteq \mathbb{N}$, existe e tal que $A = \{a \mid \langle e, a \rangle \in Q\}$. La insolubilidad del problema de la detención puede resumirse así: Q no es recursiva.

Podemos aplicar el típico argumento de diagonalización a la lista $W_0, W_1, W_2, \ldots$ de los conjuntos recursivamente numerables para generar un conjunto que no esté en ella. El conjunto

$\{a \mid a \notin W_a\}$ no puede ser igual a ninguno de los conjuntos W_q. De hecho, este conjunto no es sino $\overline{K}$, el complemento del conjunto K del teorema 36F. Como

$$q \in \overline{K} \Longleftrightarrow q \notin W_q,$$

entonces el conjunto $\overline{K}$ no puede ser igual a algún W_q; el número q es el que nos da cuenta de la diferencia entre los conjuntos $\overline{K}$ y W_q.

Y lo que es más: siempre que W_q sea un *subconjunto* recursivamente numerable de $\overline{K}$, es decir, que $W_q \subseteq \overline{K}$, podemos dar un número que pertenezca a $\overline{K}$ que no esté en W_q. Ese número es q mismo. Para ver esto, observe que no puede ser que ambos lados del bicondicional del párrafo anterior sean falsos ($q \in K$ y $q \in W_q$), ya que $W_q \subseteq \overline{K}$. Así que ambos lados son verdaderos.

El teorema 36F nos asegura que K, a pesar de ser recursivamente numerable, no es recursivo. Para demostrar la no recursividad basta mostrar que su complemento $\overline{K}$ no es recursivamente numerable. En el párrafo anterior demostramos esto de una manera particularmente fuerte; de modo que tenemos otra prueba del teorema 36F.

Llegados a este punto, podemos reconsiderar el teorema de incompletud de Gödel, desde el punto de vista computacional.

El conjunto K es recursivamente numerable (pertenece a Σ_1). De ahí se sigue (por el teorema 35K) que K es aritmético; es decir, K es definible en la estructura $\mathfrak{N}$.

Así que existe una fórmula $\kappa(v_1)$, con v_1 como única variable libre, que define K en $\mathfrak{N}$. Entonces, el conjunto $\overline{K}$ está definido en $\mathfrak{N}$ por la fórmula $\neg\kappa(v_1)$. Por lo tanto, tenemos que

$$a \in \overline{K} \Longleftrightarrow (\neg\kappa(\mathbf{S}^a\mathbf{0})) \in \mathrm{Th}\,\mathfrak{N}.$$

Esto nos muestra cómo podemos "reducir" las preguntas sobre la pertenencia al conjunto $\overline{K}$ a preguntas sobre $\mathrm{Th}\,\mathfrak{N}$. Supongamos que tenemos un número a del que quisiéramos saber si pertenece o no al conjunto $\overline{K}$. Podemos *calcular* el número $\sharp(\neg\kappa(\mathbf{S}^a\mathbf{0}))$. (De manera intuitiva está claro que efectivamente se puede calcular dicho número; formalmente podemos recurrir al inciso 5 de la sección 4 de este capítulo para asegurarnos de que es posible calcular el número *recursivamente*.) Si

tuviéramos una bola de cristal para examinar $\sharp\text{Th}\,\mathfrak{N}$ (es decir, algún truco mágico que, dado un número, nos pudiera decir si pertenece o no a $\sharp\text{Th}\,\mathfrak{N}$), entonces podríamos responder la pregunta: "¿pertenece a a $\overline{K}$?"

Pero dejemos de lado la magia. Dados A y B, conjuntos de números naturales, decimos que A es *multirreducible* a B (usando símbolos, $A \leq_m B$) sii existe una función total recursiva f tal que, para todo número a,

$$a \in A \Longleftrightarrow f(a) \in B.$$

En este sentido, el ejemplo anterior nos dice que $\overline{K} \leq_m \sharp\text{Th}\,\mathfrak{N}$. De manera más general, el argumento muestra que todo conjunto aritmético es multirreducible a $\sharp\text{Th}\,\mathfrak{N}$.

Lema 36I Supongamos que A y B son conjuntos de números naturales tales que $A \leq_m B$.

(a) Si B es recursivo, entonces A también es recursivo.

(b) Si B es recursivamente numerable, entonces A también es recursivamente numerable.

(c) Si B está en Σ_n para alguna n, entonces A también está en Σ_n para esa n.

Demostración El inciso (a) nos es muy familiar; era el inciso 2 de nuestro catálogo de la sección 3 de este capítulo, aunque con una terminología distinta.

El inciso (b) es esencialmente el mismo que (a), sólo que "con un cuantificador". Es decir, como B es recursivamente numerable, sabemos que, para alguna relación binaria recursiva Q,

$$c \in B \Longleftrightarrow \exists b\, Q(c, b).$$

Si f es una función total recursiva que multirreduce A a B, entonces, para todo número a,

$$a \in A \Longleftrightarrow f(a) \in B \Longleftrightarrow \exists b\, [Q(f(a), b)].$$

La parte entre corchetes es recursiva (es decir, $\{\langle a, b\rangle \mid Q(f(a), b)\}$ es recursivo), como la del inciso (a) de este

lema. Entonces tenemos a A descrito de modo que nos permite ver que es recursivamente numerable.

El inciso (c) es básicamente lo mismo que el inciso (a) sólo que con "n cuantificadores más" y se demuestra como el inciso (b). ⊣

La razón que tuvimos para detenernos a estudiar el conjunto particular $\overline{K}$ es que nos conduce al siguiente resultado:

Teorema de incompletud de Gödel Th$\mathfrak{N}$ no es recursivamente axiomatizable.

Demostración Th$\mathfrak{N}$ no puede ser recursivamente numerable, a menos que $\overline{K}$ lo sea, por el lema anterior. Pero toda teoría recursivamente axiomatizable es recursivamente numerable (por el inciso 20 de la sección 4 de este capítulo; también por el teorema 351). ⊣

En otras palabras: toda teoría recursivamente axiomatizable es recursivamente numerable. Pero Th$\mathfrak{N}$ no es recursivamente numerable. De modo que toda subteoría recursivamente axiomatizable debe ser incompleta.

Cuando el lector revise otra vez esta prueba, valdría la pena que sustituya las afirmaciones negativas (tal o cual conjunto *no* tiene cierta propiedad) por afirmaciones positivas.

Supongamos que T es una subteoría de Th$\mathfrak{N}$ recursivamente axiomatizable. (Entonces, por el teorema anterior, T es incompleta.) Pero nosotros quisiéramos encontrar un enunciado que demostrara directamente la incompletud.

Hemos dado una función total recursiva f que multirreduce $\overline{K}$ a $\sharp$Th$\mathfrak{N}$. A saber: $f(a) = \sharp(\neg\kappa(\mathbf{S}^a\mathbf{0}))$; entonces, para toda a,

$$a \in \overline{K} \Longleftrightarrow f(a) \in \sharp\mathrm{Th}\,\mathfrak{N}.$$

Y $f(a)$ es (el número de Gödel de) un enunciado que dice "$a \notin K$".

Considere el conjunto de números J definido de la siguiente manera:

$$a \in J \Longleftrightarrow f(a) \in \sharp T.$$

Entonces J es el conjunto de números tales que T "sabe" que no están en K. Hay dos observaciones que vale la pena hacer con respecto a J:

Primero, J es recursivamente numerable. Como es multirreducible, mediante f, al conjunto recursivamente numerable $\sharp T$, entonces se puede usar el lema 36I (b).

Segundo, $J \subseteq \overline{K}$. Tenemos que $T \subseteq \text{Th}\,\mathfrak{N}$, de modo que si T sabe que $a \notin K$, entonces verdaderamente $a \notin K$:

$$a \in J \Longleftrightarrow f(a) \in \sharp T \Longrightarrow f(a) \in \sharp \text{Th}\,\mathfrak{N} \Longleftrightarrow a \in \overline{K}.$$

Entonces J es un subconjunto recursivamente numerable de $\overline{K}$. Pero, además, es un subconjunto *propio*, pues $\overline{K}$ no es recursivamente numerable; es decir, existe un número q tal que $q \in \overline{K}$ y $q \notin J$. Por lo tanto, $f(q) \in \sharp\text{Th}\,\mathfrak{N}$, pero $f(q) \notin \sharp T$. Esto quiere decir que el enunciado $(\neg\,\kappa(\mathbf{S}^q\mathbf{0}))$ es verdadero (en $\mathfrak{N}$) pero no está en T, con lo que finalmente hemos demostrado la incompletud de T.

Sin embargo, ¿qué es lo que nos "dice" ese enunciado? Podemos tomar cualquier número q tal que $W_q = J$. Entonces $q \in \overline{K}$ y $q \notin J$.

En ese caso tendríamos que:

$$\begin{array}{ll} (\neg\,\kappa(\mathbf{S}^q\mathbf{0})) & \text{dice } q \notin K \\ & \textit{i.e. } q \notin W_q \\ & \textit{i.e. } q \notin J \quad \text{ya que } W_q = J \\ & \textit{i.e. } f(q) \notin \sharp T \quad \text{por la definición de } J \\ & \textit{i.e. } T \nvdash (\neg\,\kappa(\mathbf{S}^q\mathbf{0})). \end{array}$$

El enunciado que construimos para dar cuenta de la incompletud de T afirma la imposibilidad de que él mismo sea demostrable a partir de la teoría axiomatizable T.

Después de todo, el argumento de computabilidad y el argumento de autorreferencia para la prueba del teorema de incompletud de Gödel no son tan distintos. De hecho, el argumento de computabilidad es bastante cercano al argumento de diagonalización (de la sección cero de este capítulo), sólo que el método de diagonalización se usa en un contexto distinto.

Reducción de los problemas de decisión[3]

Supongamos que tenemos una función parcial recursiva binaria f. Entonces afirmamos que, por ejemplo, la función g definida como:

$$g(a) = f(3,a)$$

también es una función parcial recursiva. Esto queda claro, al menos desde un punto de vista intuitivo, ya que g se puede calcular tomando 3 como valor de la primera variable y luego siguiendo las instrucciones para f. Si este argumento se formaliza, se puede tener una prueba rigurosa. Existe una fórmula $\varphi = \varphi(v_1, v_2, v_3)$ que representa débilmente a f (como relación) en $\mathrm{Cn}A_{\mathcal{E}}$. Entonces g está débilmente representada por $\varphi(\mathbf{S}^3 0, v_1, v_2)$, suponiendo que v_1 y v_2 son sustituibles por v_2 y v_3 en φ. (Si esto no sucede, siempre se puede usar una variante alfabética de φ.)

A primera vista, esto no dice mucho. Sin embargo, si miramos con cuidado, encontraremos que se trata de un resultado sutil muy interesante. Hemos podido transformar las instrucciones para f en instrucciones para g. De manera que, dado un índice para f y el número 3, existe una función recursiva que nos da el índice de g. La versión del resultado que presentamos a continuación suele conocerse con el críptico nombre de "teorema S-m-n".

Teorema del parámetro Para cada $m \geq 1$ y $n \geq 1$, existe una función recursiva ρ tal que, para cualesquiera $e, \vec{a}, \vec{b}$,

$$[[e]]_{m+n}(a_1, \ldots, a_m, b_1, \ldots, b_n) = [[\rho(e, a_1, \ldots, a_m)]]_n\,(b_1, \ldots, b_n).$$

(Está claro que, en este caso, la igualdad quiere decir que si uno de los lados está definido, entonces el otro lado también lo está, y que los valores coinciden. A veces se usa el símbolo "$\simeq$" para designar esta relación.)

Del lado izquierdo de la ecuación, $\vec{a}$ es un valor asignado a las variables de la función $[[e]]_{m+n}$; del lado derecho, en cambio, $\vec{a}$ consiste de parámetros de los que depende la función

[3] En una primera lectura, el lector puede omitir lo que queda de esta sección.

$[[\rho(e,\vec{a})]]_n$. En nuestro ejemplo, teníamos que $m = n = 1$ y $a_1 = 3$. Como ρ depende de m y n, parece más lógico usar como notación "ρ_n^m". Pero nosotros seguiremos usando simplemente "ρ".

Demostración para $m = n = 1$ Se podría hacer una demostración apegada a lo que se dijo antes de enunciar el teorema. Sin embargo, para evitar tener que lidiar con variantes alfabéticas, seguiremos una estrategia ligeramente distinta.

Gracias al teorema de la forma normal sabemos que una función parcial de tres argumentos h, definida de la siguiente manera:

$$h(e, a, b) = [[e]]_2(a, b)$$

es una función parcial recursiva. Por lo tanto, existe una fórmula ψ que representa débilmente h (como relación). Podemos suponer que v_1 y v_2 no están cuantificadas en ψ. De modo que podemos tomar

$$\begin{aligned}\rho(e, a) &= \sharp\psi(\mathbf{S}^e0, \mathbf{S}^a0, v_1, v_2)\\ &= \mathrm{Sb}(\mathrm{Sb}(\mathrm{Sb}(\mathrm{Sb}(\sharp\psi, \sharp v_1, \sharp\mathbf{S}^e0), \sharp v_2, \sharp\mathbf{S}^a0), \sharp v_3, \sharp v_1), \sharp v_4, \sharp v_2).\end{aligned}$$

Entonces $\rho(e, a)$ es el número de Gödel de una fórmula que representa débilmente a la función $g(b) = [[e]]_2(a, b)$. Por lo tanto, es un índice de g. ⊣

Utilizaremos el teorema del parámetro para demostrar que ciertos conjuntos *no* son recursivos. Ya sabemos que $K = \{a \mid [[a]]_1(a) \text{ está definida}\}$ no es recursivo. Dado un conjunto no recursivo A, a veces es posible encontrar una función (total) recursiva g tal que:

$$a \in K \Leftrightarrow g(a) \in A$$

o una función (total) recursiva g' tal que

$$a \notin K \Leftrightarrow g'(a) \in A.$$

En ambos casos se sigue que A no puede ser recursivo, pues K no lo es. En el primer caso tenemos que $K \leq_m A$ y A no

pertenece a Π_1 (por el lema 36I); en el segundo caso, $\overline{K} \leq_m A$ y A no pertenece a Σ_1. Así que, en ambos casos, A no es recursivo. Generalmente, las funciones g o g' pueden obtenerse a partir del teorema del parámetro.

Ejemplo $\{a \mid W_a = \emptyset\}$ no es recursivo.

Demostración Llamemos a dicho conjunto A. Lo primero es observar que $A \in \Pi_1$, ya que $W_a = \emptyset$ sii $\forall b\, \forall k\ \langle a, b, k\rangle \notin T_1$. Así que K no puede ser multirreducible a A; sin embargo, parece razonable esperar que $\overline{K}$ lo sea. Es decir, queremos encontrar una función total recursiva g tal que

$$[\![a]\!]_1(a) \text{ está indefinida } \Leftrightarrow \operatorname{dom}[\![g(a)]\!]_1 = \emptyset.$$

Esto se cumple si para toda b, $[\![g(a)]\!]_1(b) = [\![a]\!]_1(a)$. Así que conviene comenzar con la función parcial recursiva

$$f(a, b) = [\![a]\!]_1(a)$$

y sea $g(a) = \rho(\hat{f}, a)$, donde $\hat{f}$ es un índice de f. Entonces

$$[\![g(a)]\!]_1(b) = [\![\rho(\hat{f}, a)]\!]_1(b) = f(a,b) = [\![a]\!]_1(a).$$

Así que g muestra que $\overline{K}$ es multirreducible a A. ⊣

Teorema 36J (Rice, 1953) Sea $\mathcal{C}$ un conjunto de funciones parciales recursivas de un argumento. Entonces el conjunto $\{e \mid [\![e]\!]_1 \in \mathcal{C}\}$ de índices de los elementos de $\mathcal{C}$ es recursivo sii o bien $\mathcal{C}$ es vacío, o bien contiene todas las funciones parciales recursivas de un argumento.

Demostración Sólo necesitamos demostrar un lado del bicondicional. Sea $I_{\mathcal{C}} = \{e \mid [\![e]\!]_1 \in \mathcal{C}\}$ el conjunto de índices de los elementos de $\mathcal{C}$.

Caso I: La función vacía $\emptyset$ no está en $\mathcal{C}$. Si no hay nada en $\mathcal{C}$, entonces terminamos; pero supongamos que hay una función ψ que está en $\mathcal{C}$. Podemos demostrar que K es multirreducible a $I_{\mathcal{C}}$ si tenemos una función total

recursiva g tal que

$$[[g(a)]]_1 = \begin{cases} \psi & \text{si } a \in K, \\ \emptyset & \text{si } a \notin K. \end{cases}$$

En ese caso, $a \in K \Leftrightarrow [[g(a)]]_1 \in C \Leftrightarrow g(a) \in I_C$.

Podemos obtener g a partir del teorema del parámetro si tomamos

$$g(a) = \rho(e,a),$$

donde

$$[[e]]_2(a,b) = \begin{cases} \psi(b) & \text{si } a \in K, \\ \text{indefinido} & \text{si } a \notin K. \end{cases}$$

La anterior es una función parcial recursiva, ya que

$$[[e]]_2(a,b) = c \Leftrightarrow a \in K \quad \text{y} \quad \psi(b) = c$$

y el lado derecho de este bicondicional es recursivamente numerable.

Caso II: $\emptyset \in C$. Entonces el complemento de C, que denotamos con $\overline{C}$, cae dentro del caso I, de donde podemos concluir que $I_{\overline{C}}$ no es recursivo. Pero $I_{\overline{C}}$ es el complemento de I_C, así que I_C no puede ser recursivo.

Por lo tanto, I_C no es recursivo en ninguno de ambos casos. ⊣

Ejemplos Como consecuencia del teorema de Rice tenemos que, para toda e fija, el conjunto $\{a \mid W_a = W_e\}$ no es recursivo. En particular, $\{a \mid W_a = \emptyset\}$ no es recursivo, como ya se había probado antes. Los siguientes resultados también provienen del teorema de Rice: los conjuntos $\{a \mid W_a \text{ es infinito}\}$ y $\{a \mid W_a \text{ es recursivo}\}$ no son recursivos.

Máquinas registradoras

Existen diversas definiciones equivalentes para la clase de las funciones recursivas; muchas de esas definiciones se refieren

a aparatos de cómputo ideales. Estos aparatos se parecen a las computadoras digitales, pero sin restricciones de espacio de memoria. En 1936, Alan Turing publicó la primera definición de este tipo y, casi al mismo tiempo, Emil Post realizó un trabajo similar. Nosotros veremos aquí la versión de Shepherdson y Sturgis (1963).

Una *máquina registradora* tiene un número finito de registros, numerados $1, 2, \ldots, K$. Cada registro puede almacenar un número natural, sin importar cuán grande sea. El funcionamiento de la máquina depende de un *programa,* que no es sino una sucesión finita de *instrucciones* que se toman de la siguiente lista:

I r (con $1 \leq r \leq K$). "Incrementar r." Con esta instrucción se suma 1 al número del registro r. La máquina pasa después a la siguiente instrucción del programa.

D r (con $1 \leq r \leq K$). "Disminuir r." Esta instrucción depende del contenido del registro r. Si el número en el registro r es distinto de cero, entonces se le resta 1 y en lugar de pasar a la siguiente instrucción, se pasa a la que está después de ésta. Sin embargo, si dicho número es cero, la máquina pasa, sin más, a la siguiente instrucción. En resumen: la máquina trata de disminuir el número que hay en r, y si lo logra, entonces se salta una instrucción.

T q (donde q es un entero positivo, negativo o cero). "Transferir q." Todos los registros se quedan como están. La máquina pasa a la q-ésima instrucción a partir de la que está (si $q \geq 0$) o a la instrucción que está $|q|$ lugares antes de ésta (si $q < 0$). La máquina se detiene si en el programa no existe dicha instrucción. La instrucción T0 no es sino un ciclo en el que la máquina repite una y otra vez esta instrucción.

EJEMPLOS

1. Programa para vaciar el registro 7.

D	7	Tratar de disminuir lo que hay en 7.
T	2	
T	−2	Ir hacia atrás y repetir.
		Detener.

2. Programa para trasladar el número del registro r al registro s.

Vaciar el registro s		(Usar el programa del primer ejemplo.)
→D	r	Restar 1 al número en r.
T	3	Detener cuando se llegue al cero.
I	s	Sumar 1 al número en s.
T	−3	Repetir

Este programa tiene un total de siete instrucciones y deja un cero en el registro r.

3. Programa para sumar el registro 1 a los registros 2 y 3.

→D	1
T	4
I	2
I	3
T	−4

4. (Suma) Supongamos que a y b están en los registros 1 y 2, respectivamente. Quisiéramos tener $a + b$ en el registro 3, pero manteniendo a y b en los registros 1 y 2.

	Contenidos de los registros			
Vaciar el registro 3.	a	b	0	
Trasladar el número del registro 1 al registro 4.	0	b	0	a
Sumar el registro 4 a los registros 1 y 3.	a	b	a	0
Trasladar el número del registro 2 al registro 4.	a	0	a	b
Sumar el registro 4 a los registros 2 y 3.	a	b	$a + b$	0

Tal como está escrito, este programa da como resultado 27 instrucciones, aunque en realidad tres de ellas son innecesarias. (En el cuarto enunciado se comienza con una instrucción para vaciar el registro 4, que ya está limpio.) Al final tenemos de nuevo el número a en el registro 1. Sin embargo, a lo largo del programa es necesario vaciar el registro 1; ésta es la única forma en que se puede determinar el número a.

5. (Resta) Sean $a \dot{-} b = \max(a - b, 0)$. Dejamos al lector la elaboración de este programa (ejercicio 11).

Supongamos ahora que f es una función n-aria sobre $\mathbb{N}$. Posiblemente existirá un programa P tal que, si construimos una máquina registradora (que tenga los registros a los que se refiere P) con $a_1, \ldots, a_n$ en los registros $1, \ldots, n$ y aplicamos el programa P, se cumplen las siguientes condiciones:

(i) Si $f(a_1, \ldots, a_n)$ está definido, entonces su cálculo termina con $f(a_1, \ldots, a_n)$ en el registro $n + 1$. Además, el cálculo termina cuando se busca una instrucción $(p + 1)$, donde p es igual a la longitud de P.

(ii) Si $f(a_1, \ldots, a_n)$ está indefinido, entonces el cómputo nunca termina.

Si existe dicho programa P, entonces decimos que P *calcula* f.

Teorema 36K Sea f una función parcial. Entonces existe un programa que calcula f sii f es una función parcial recursiva.

De modo que a partir de las máquinas registradoras podemos obtener la clase de las funciones parciales recursivas, una clase que originalmente se definió en términos de la representabilidad en teorías consistentes finitamente axiomatizables. El hecho de que se tengan dos formas tan distintas de determinar la misma clase de funciones parciales da cuenta de la importancia que tiene esta clase.

Esbozo de la demostración Para demostrar que las funciones calculables mediante máquinas registradoras son funciones

parciales recursivas hay que "aritmetizar los cálculos", con el mismo espíritu con el que se aritmetizaron las deducciones en la sección 4 de este capítulo. Es decir, hay que asignar números de Gödel a los programas y a las sucesiones de configuraciones de memoria. Entonces hay que verificar que todos los conceptos relevantes, que se traducen a relaciones numéricas mediante la numeración de Gödel, sean recursivos. (Al final, esto permite entender, desde un punto vista más general, que en realidad las deducciones y los cálculos son el mismo tipo de objeto.)

Por otro lado, para demostrar que las funciones parciales recursivas son calculables mediante máquinas registradoras, se puede hacer lo mismo que se hizo en las secciones 3 y 4 de este capítulo, pero, en lugar de demostrar que cada una de las posibles funciones son representables en Cn A_E, hay que probar que son calculables mediante máquinas registradoras. Esto es más sencillo de lo que parece, porque después de algunas páginas queda claro que las demostraciones se repiten. Es posible explicar este ciclo, ya que se puede demostrar que la clase de todas las funciones recursivas se genera a partir de unas cuantas funciones recursivas, mediante el operador composición (definido en el teorema 33L) y el operador "mínimo cero" (teorema 33M). Buena parte del trabajo de las secciones 3 y 4 tiene que ver con la demostración de este hecho. De modo que, una vez que se demuestra que las funciones de este conjunto básico son calculables mediante una máquina registradora y que la clase de las funciones calculables mediante máquinas registradoras es cerrada bajo composición y el operador "mínimo-cero", se puede repetir el mismo trabajo una y otra vez hasta obtener que todas las funciones recursivas son calculables. ⊣

Ejercicios

1. Sean f y g las siguientes funciones:

$$f(n) = \begin{cases} 0 & \text{si la conjetura de Goldbach} \\ & \text{es verdadera,} \\ 1 & \text{en caso contrario;} \end{cases}$$

$$g(n) = \begin{cases} 0 & \text{si en la expansión decimal de } \pi \text{ hay,} \\ & \text{en algún punto, una sucesión} \\ & \text{de al menos } n \text{ sietes consecutivos,} \\ 1 & \text{el caso contrario.} \end{cases}$$

¿Es f recursiva? ¿Es g recursiva? (La conjetura de Goldbach dice que todo entero par mayor que 2 es la suma de dos primos. En la primera edición de este libro, usamos para este caso el último teorema de Fermat.)

2. Definimos la función "diagonal" como

$$d(a) = [[a]]_1(a) + 1.$$

   (a) Muestre que d es una función parcial recursiva.

   (b) Por el inciso (a) tenemos que $d = [[e]]_1$ para algún número e. De modo que, por un lado, $d(e) = [[e]]_1(e)$, y, por el otro, $d(e) = [[e]]_1(e) + 1$. Pero, entonces, ¿se puede cancelar para concluir que $0 = 1$? *Sugerencia:* use el símbolo especial "$\simeq$" para decir que o bien ambos lados de la ecuación están indefinidos, o bien que están definidos y son iguales. Reescriba el argumento con esta notación.

3. (a) Demuestre que el rango de cualquier función parcial recursiva es recusivamente numerable.

   (b) Demuestre que el rango de una función total recursiva f estrictamente creciente (es decir, $f(n) < f(n+1)$) es recursivo.

   (c) Demuestre que el rango de una función total recursiva f no decreciente (es decir, $f(n) \leq f(n+1)$) es recursivo.

4. (a) Sea A un subconjunto no vacío y recursivamente numerable de $\mathbb{N}$. Demuestre que A es el rango de alguna función total recursiva.
   (b) Demuestre que todo subconjunto infinito de $\mathbb{N}$ recursivamente numerable contiene un conjunto infinito recursivo.
5. Muestre que toda función parcial recursiva tiene una cantidad infinita de índices.
6. Dé un ejemplo de una función f y un número e tales que, para toda a,

$$f(a) = U(\mu k\ \langle e,a,k\rangle \in T_1),$$

pero donde e no es el número de Gödel de una fórmula que represente débilmente a f en Cn A_E.

7. Muestre que el teorema del parámetro puede reforzarse pidiendo que ρ sea inyectiva.
8. Recuerde que la unión de dos conjuntos recursivamente numerables es recursivamente numerable (ejercicio 7 de la sección 5 de este capítulo). Muestre que existe una función total recursiva g tal que $W_{g(a,b)} = W_a \cup W_b$.
9. Muestre que $\{a \mid W_a$ tiene dos o más elementos$\}$ está en Σ_1, pero no en Π_1.
10. Muestre que no hay un conjunto recursivamente numerable A tal que $\{[[a]]_1 \mid a \in A\}$ sea igual a la clase de las funciones totales recursivas en $\mathbb{N}$.
11. Formule los programas de máquinas registradoras que permitan calcular las siguientes funciones:
    (a) Resta, $a \dot{-} b = \max(a - b, 0)$.
    (b) Multiplicación, $a \cdot b$.
    (c) $\max(a, b)$.
12. Suponga que existe un programa de máquina registradora que calcula una función parcial f de n argumentos. Muestre que dados cualesquiera enteros $r_1, \ldots, r_n$ (todos

distintos), p y k, podemos encontrar un programa Q tal que cada vez que se inserte en una máquina registradora (que tenga todos los registros a los que Q se refiere) $a_1, \ldots, a_n$ en los registros $r_1, \ldots, r_n$ y se aplique el programa Q, entonces (i) si $f(a_1, \ldots, a_n)$ está definido, entonces el cálculo termina con $f(a_1, \ldots, a_n)$ en el registro p, y los contenidos de los registros $1, 2, \ldots, k$ son los mismos que al principio (excepto para el registro p); además, el cálculo termina cuando se busca la instrucción $(q + 1)$, donde q es la longitud de Q; (ii) si $f(a_1, \ldots, a_n)$ está indefinida, entonces el cálculo nunca termina.

13. Sea $g : \mathbb{N}^{n+1} \rightarrow \mathbb{N}$ una función (total) que se puede calcular con un programa de máquina registradora. Sea $f(a_1, \ldots, a_n) = \mu b[g(a_1, \ldots, a_n, b) = 0]$, donde el lado derecho queda indefinido si dicha b no existe. Muestre que la función parcial f puede calcularse con algún programa de máquina registradora.

14. Muestre que los siguientes conjuntos efectivamente tienen el lugar que se les asocia en la jerarquía aritmética. (En cada caso, el lugar asignado es el mejor que podrían tener, pero no demostraremos este hecho.)
    (a) $\{e \mid [[e]]_1$ es total$\}$ está en Π_2.
    (b) $\{e \mid W_e$ es finito$\}$ está en Σ_2.
    (c) $\{e \mid W_e$ es cofinito$\}$ está en Σ_3.
    (d) $\{e \mid W_e$ es recursivo$\}$ está en Σ_3.

15. Sea $Tot = \{e \mid [[e]]_1$ es total$\}$. Está claro que $Tot \subset K$. Muestre que no existe ningún conjunto recursivo A tal que:
$$Tot \subseteq A \subseteq K.$$
Observación: Este resultado incluye los teoremas 36E y 36F, así que las pruebas dadas entonces se pueden adaptar para este caso.

16. (a) Muestre que todo conjunto Π_2 de números naturales es, para algún número e, el conjunto:
$$\{a \mid \forall b \, \exists c \; T_2(e, a, b, c)\}.$$

(b) Muestre que el conjunto $\{a \mid \text{no } \forall b\ \exists c\ T_2(a,a,b,c)\}$ es Σ_2, pero no es Π_2.

*(c) Generalice los incisos (a) y (b) para demostrar que, para toda n, existe un conjunto que es Σ_n, pero no es Π_n.

17. Suponga que A es un conjunto de números naturales que es aritmético, pero que no es Π_m. Utilice el argumento previo al lema 36I para demostrar que $\sharp\text{Th}\,\mathfrak{N}$ no es Σ_m.

Observación: Los ejercicios 16 y 17 dan una demostración del teorema de Tarski (que dice que $\sharp\text{Th}\,\mathfrak{N}$ no es aritmético) a partir de la teoría computacional.

7. *Segundo teorema de incompletud*

Regresemos una vez más al inciso 20 de la sección 4 de este capítulo. Supongamos que tenemos una teoría T recursivamente axiomatizable, dada a partir de un conjunto recursivo de axiomas A (es decir, $\sharp A$ es recursivo). Tenemos entonces, como en el inciso 20, que:

$a \in \sharp T \iff \exists d[d$ es el número de una deducción a partir de A y el último componente de d es a y a es el número de Gödel de un enunciado].

El conjunto de pares $\langle a,d\rangle$ que cumplen con las condiciones entre corchetes es recursivo. Sea $\pi(v_1,v_2)$ una fórmula —elegida de una forma más o menos natural— que represente numéricamente esa relación binaria en A_E.

Dado un enunciado σ, podemos expresar "$T \vdash \sigma$" mediante el enunciado $\exists v_2\ \pi(\mathbf{S}^{\sharp\sigma}\mathbf{0}, v_2)$. Pero démosle un nombre a dicho enunciado, digamos que

$$\text{Dem}_T\,\sigma = \exists v_2\ \pi(\mathbf{S}^{\sharp\sigma}\mathbf{0}, v_2).$$

(Aquí Dem abrevia "demostrable". Tal vez el subíndice debería ser "A" en lugar de "T", ya que la recursividad del conjunto A de axiomas se utilizará en la construcción del enunciado.)

Lema 37A Sea T una teoría recursivamente axiomatizable como la de antes.

(a) Siempre que $T \vdash \sigma$ tenemos que $A_E \vdash \text{Dem}_T\sigma$.

(b) Si además tenemos que T contiene A_E, entonces T tiene la propiedad de "reflexión":

$$T \vdash \sigma \Longrightarrow T \vdash \text{Dem}_T\sigma.$$

Demostración Si $T \vdash \sigma$, entonces sea d el número de una deducción de σ a partir de los axiomas A para T. Tenemos que $A_E \vdash \pi(\mathbf{S}^{\sharp\sigma}\mathbf{0}, \mathbf{S}^d\mathbf{0})$ y, por lo tanto, que $A_E \vdash \text{Dem}_T\sigma$. Con esto demostramos el inciso (a), del que se sigue inmediatamente el inciso (b). ⊣

De modo que, bajo supuestos muy sencillos, siempre que T demuestre un enunciado, al mismo tiempo *sabe* que lo demuestra. Obsérvese que el inciso (b) *no* dice que $T \vdash (\sigma \to \text{Dem}_T\sigma)$. Por ejemplo, si σ es verdadero (en $\mathfrak{N}$), pero no se puede demostrar a partir de A_E, entonces el enunciado $(\sigma \to \text{Dem}_{A_E}\sigma)$ *no* se puede demostrar a partir de A_E y, de hecho, es falso en $\mathfrak{N}$.

Regresando a la demostración del teorema de incompletud de Gödel (mediante el argumento de autorreferencia), podemos usar el lema del punto fijo para obtener un enunciado σ que nos hable de su propia indemostrabilidad en T:

$$A_E \vdash (\sigma \leftrightarrow \neg\,\text{Dem}_T\,\sigma).$$

El siguiente lema nos da parte del teorema de incompletud (la otra parte se encuentra en el ejercicio 2 de la sección 5 de este capítulo):

Lema 37B Sea T una teoría recursivamente axiomatizable que contiene A_E y sea σ el enunciado antes obtenido mediante el lema del punto fijo. Si T es consistente, entonces $T \nvdash \sigma$.

Demostración

$$\begin{aligned} T \vdash \sigma &\Rightarrow T \vdash \text{Dem}_T\sigma && \text{por reflexión} \\ &\Rightarrow T \vdash \neg\sigma && \text{por la elección de } \sigma \end{aligned}$$

de modo que T sería inconsistente. ⊣

Podemos decir que este lema tan sólo refleja las ideas que se usaron en la sección 5 de este capítulo, y la demostración del lema 37B no era demasiado compleja. Pero justamente ése es el punto: como la demostración *no* es demasiado compleja, entonces tal vez se puede llevar a cabo *dentro de* la teoría T, si T es "suficientemente fuerte". Es decir, podemos esperar que los pasos

$$\begin{aligned}\text{Dem}_T\sigma &\to \text{Dem}_T\text{Dem}_T\sigma\\ &\to \text{Dem}_T\neg\sigma\\ &\to \text{Dem}_T\mathbf{0} = \mathbf{S0}\end{aligned}$$

puedan llevarse a cabo en una extensión lo suficientemente fuerte T de A_E.

En caso de que esto se pueda hacer, entonces tendremos una conclusión muy interesante. Sea Cons T el enunciado $\neg\text{Dem}_T\mathbf{0} = \mathbf{S0}$, que indirectamente nos dice "T es consistente". (Se eligió el enunciado $\mathbf{0} = \mathbf{S0}$ simplemente por ser un enunciado claramente refutable a partir de A_E.) Si T nos permite llevar a cabo los pasos expuestos en el párrafo anterior, entonces podemos concluir que:

$$T \nvdash \text{Cons}\, T, \quad \text{a menos que } T \text{ sea } \textit{in}\text{consistente.}$$

(Desde luego, una teoría inconsistente contiene todos los enunciados, incluidos aquellos que afirman, falsamente, que la teoría es consistente. Lo que tenemos entonces aquí es que, bajo supuestos adecuados, ésta es la *única* forma en que una teoría puede demostrar su propia consistencia.) Veamos esto con detalle: supongamos que $T \vdash$ Cons T. Entonces, por el párrafo anterior, $T \vdash \neg\text{Dem}_T\sigma$. Pero gracias a la forma en que se eligió σ, tenemos que $T \vdash \sigma$ y entonces podemos usar el lema 37B.

Para ser más precisos, diremos que T es *suficientemente fuerte* si cumple las siguientes tres condiciones de "derivación":

1. $A_E \subseteq T$. Esto implica, por el lema 37A, que T tiene la propiedad de reflexión, $T \vdash \sigma \Rightarrow T \vdash \text{Dem}_T\,\sigma$.

2. Para todo enunciado σ, $T \vdash (\text{Dem}_T\sigma \to \text{Dem}_T\text{Dem}_T\sigma)$. Ésta también es la propiedad de reflexión, sólo que formalizada dentro de T.

3. Para cualesquiera enunciados ρ y σ, $T \vdash (\text{Dem}_T(\rho \to \sigma) \to (\text{Dem}_T\rho \to \text{Dem}_T\sigma))$. Esto es el modus ponens, formalizado dentro de T.

Lema 37B formalizado Supongamos que T es un teoría recursivamente axiomatizable y suficientemente fuerte. Sea σ un enunciado tal que:

$$A_E \vdash (\sigma \leftrightarrow \neg \text{Dem}_T\sigma).$$

Entonces $T \vdash (\text{Cons}\, T \to \neg \text{Dem}_T\, \sigma)$.

Demostración Basta poner, con mucho cuidado, todas las piezas juntas. Por la forma en que se eligió σ tenemos que:

$$T \vdash (\sigma \to (\text{Dem}_T\sigma \to \mathbf{0} = \mathbf{S0})).$$

Si primero aplicamos reflexión y después modus ponens formalizado a esta fórmula, obtendremos

$$T \vdash (\text{Dem}_T\sigma \to \text{Dem}_T(\text{Dem}_T\sigma \to \mathbf{0} = \mathbf{S0})),$$

a partir de lo cual podemos volver a aplicar modus ponens formalizado y obtener

$$T \vdash (\text{Dem}_T\sigma \to (\text{Dem}_T\text{Dem}_T\sigma \to \neg\, \text{Cons}\, T)).$$

Esta fórmula (a la derecha del símbolo $\vdash$), junto con $\text{Dem}_T\sigma \to \text{Dem}_T\text{Dem}_T\sigma$ (reflexión formalizada), implica por lógica de enunciados que $\text{Dem}_T\sigma \to \neg\, \text{Cons}\, T$. ⊣

Segundo teorema de incompletud de Gödel (1931) Supongamos que T es una teoría recursivamente axiomatizable y suficientemente fuerte. Entonces $T \vdash \text{Cons}\, T$ si y sólo si T es *in*consistente.

Demostración Si $T \vdash \text{Cons}\, T$ entonces, por el lema 37B formalizado, tenemos que $T \vdash \neg\, \text{Dem}_T\, \sigma$. Pero, por la manera como se eligió σ, tendríamos entonces que $T \vdash \sigma$. Entonces, a partir del lema 37B (informal), concluimos que T es inconsistente. ⊣

Es posible sacar más provecho de estas ideas. El lema 37B puede verse como un caso especial (con τ igual a $\mathbf{0} = \mathbf{S0}$) del siguiente resultado:

Lema 37C Sea T una teoría recursivamente axiomatizable que contiene A_E, sea τ un enunciado y σ el enunciado que se obtiene a partir del lema del punto fijo, de modo que

$$A_E \vdash (\sigma \leftrightarrow (\mathrm{Dem}_T\sigma \rightarrow \tau)).$$

Si $T \vdash \sigma$, entonces $T \vdash \tau$.

Demostración Intuitivamente lo que σ dice es "Si soy demostrable, entonces τ". Si $T \vdash \sigma$, entonces por reflexión tenemos que $T \vdash \mathrm{Dem}_T\sigma$. Y luego por la elección de σ, tendríamos que $T \vdash \tau$. ⊣

En realidad lo que nos interesa no es este lema, sino su versión formalizada:

Lema 37C formalizado Supongamos que T es una teoría recursivamente axiomatizable y suficientemente fuerte. Sea τ un enunciado y σ un enunciado tal que

$$A_E \vdash (\sigma \leftrightarrow (\mathrm{Dem}_T\sigma \rightarrow \tau)).$$

Entonces $T \vdash \mathrm{Dem}_T\sigma \rightarrow \mathrm{Dem}_T\tau)$.

Demostración Procedemos como antes. Por la elección de σ tenemos que

$$T \vdash (\sigma \rightarrow (\mathrm{Dem}_T\sigma \rightarrow \tau)).$$

Si aplicamos a esta fórmula primero reflexión y después modus ponens formalizado, obtendremos

$$T \vdash (\mathrm{Dem}_T\sigma \rightarrow \mathrm{Dem}_T(\mathrm{Dem}_T\sigma \rightarrow \tau)),$$

a partir de lo cual podemos aplicar otra vez modus ponens formalizado y obtener

$$T \vdash (\mathrm{Dem}_T\sigma \rightarrow (\mathrm{Dem}_T\mathrm{Dem}_T\sigma \rightarrow \mathrm{Dem}_T\tau)).$$

Esta fórmula, a la derecha del símbolo $\vdash$, junto con $\mathrm{Dem}_T\sigma \rightarrow \mathrm{Dem}_T\mathrm{Dem}_T\sigma$ (reflexión formalizada), implica, por lógica de enunciados, que $\mathrm{Dem}_T\sigma \rightarrow \mathrm{Dem}_T\tau$. ⊣

Teorema de Löb (1955) Supongamos que T es una teoría recursivamente axiomatizable y suficientemente fuerte. Si τ es un enunciado tal que $T \vdash (\text{Dem}_T\tau \to \tau)$, entonces $T \vdash \tau$.

Está claro que si $T \vdash \tau$, entonces $T \vdash (\rho \to \tau)$ para cualquier enunciado ρ. De modo que la conclusión del teorema de Löb se puede reescribir de la siguiente manera:

$$T \vdash (\text{Dem}_T\tau \to \tau) \iff T \vdash \tau.$$

Demostración Dado un enunciado τ, construimos un enunciado σ que diga "Si soy demostrable, entonces τ", como se hizo antes. Supongamos que $T \vdash (\text{Dem}_T\tau \to \tau)$. Por el lema 37C formalizado tenemos que $T \vdash (\text{Dem}_T\sigma \to \text{Dem}_T\tau)$. Entonces, gracias a la forma en que se eligió σ, podemos concluir que $T \vdash \sigma$. De modo que, por el lema 37C (informal), tenemos que $T \vdash \tau$. ⊣

El teorema de Löb surgió originalmente como una forma de resolver el problema del ejercicio 1; sin embargo, implica el segundo teorema de incompletud de Gödel (y de alguna manera es equivalente a él). Supongamos que T es una teoría axiomatizable suficientemente fuerte. Si usamos el teorema de Löb con τ igual a $0 = \mathbf{S}0$, tenemos que

$$T \vdash (\text{Dem}_T(0 = \mathbf{S}0) \to 0 = \mathbf{S}0) \Rightarrow T \vdash 0 = \mathbf{S}0,$$

es decir,

$$T \vdash \text{Cons}\, T \Rightarrow T \text{ es inconsistente.}$$

De modo que obtenemos una demostración para el segundo teorema de incompletud.

Pero hay algo que todavía no hemos discutido: ¿Qué teorías *son* suficientemente fuertes? ¿Existe alguna (más allá del caso trivial de una teoría inconsistente)? No sólo podemos decir que sí las hay, sino que aquí daremos dos. La primera se llama "aritmética de Peano" (AP). Sus axiomas son los axiomas de A_E junto con todos los "axiomas de inducción". Estos últimos son las cerraduras universales de las fórmulas de tipo

$$\varphi(0) \land \forall x(\varphi(x) \to \varphi(\mathbf{S}x)) \to \forall x\, \varphi(x),$$

donde φ es una fórmula. Los axiomas de inducción —que establecen el principio de inducción matemática común y corriente— nos permiten obtener muchos resultados dentro de la aritmética de Peano (por ejemplo, la ley conmutativa de la suma). Pero, para convencerse de que la reflexión formalizada y el modus ponens formalizado se pueden derivar en la aritmética de Peano, es necesario desarrollar los detalles, cosa que no haremos aquí.

Sabemos que la aritmética de Peano es consistente porque es verdadera en $\mathfrak{N}$; sin embargo, por el segundo teorema de incompletud, AP no puede demostrar su propia consistencia. Nosotros "sabemos" que AP es consistente gracias a un argumento matemático informal, o —si se quiere— gracias a un argumento dentro de la teoría de conjuntos. Así que la teoría de conjuntos tiene más "capacidad de demostración" que AP, ya que prueba la consistencia de AP, mientras que AP no lo puede hacer.

Una segunda teoría suficientemente fuerte es la teoría axiomática de conjuntos. Para ser más precisos, se trata del conjunto de enunciados del lenguaje de la teoría de números que se pueden demostrar en la teoría axiomática de conjuntos. En la siguiente subsección veremos esto con detalle. La ventaja de esta teoría es que parece bastante creíble que tanto la reflexión formalizada como el modus ponens formalizado se pueden derivar a partir de ella (al menos desde un punto de vista intuitivo). Pero ¿qué nos hace creer que la teoría de conjuntos es consistente? Sabemos que AP es consistente porque es verdadera en el "modelo estándar" $\mathfrak{N}$ de la teoría de números; sin embargo, no está nada claro que sea posible concebir un "modelo estándar de la teoría de conjuntos".

Aplicaciones a la teoría de conjuntos

Sabemos que, dentro del lenguaje de la teoría de números, Cn A_E es incompleta y no recursiva, como sucede con cualquier teoría recursivamente axiomatizable de ese lenguaje.

Pero dejemos de lado la aritmética y concentrémonos en la teoría de conjuntos. En este caso tenemos un lenguaje (con los parámetros $\forall$ y $\in$) y un conjunto de axiomas. Todos los

conjuntos de axiomas que han sido aceptados hasta ahora son recursivos. Para ser más precisos, el conjunto de números de Gödel de dichos axiomas es recursivo. De modo que la teoría (de conjuntos) que se obtiene es recursivamente numerable. Nosotros afirmamos que si esta teoría es consistente, entonces no es recursiva y, por lo tanto, tampoco completa. A continuación daremos una idea general del argumento. En un sentido muy real, es posible insertar el lenguaje de la teoría de números en la teoría de conjuntos. Una vez hecho eso, podemos fijarnos en el fragmento de la teoría de conjuntos que tiene que ver con los números naturales y su aritmética (la parte sombreada de la figura 14); se trata de una teoría compatible con A_E y, por lo tanto, no recursiva. Ahora bien, si la teoría de conjuntos fuera recursiva, entonces su parte aritmética también tendría que serlo, pero no lo es. Como resultado adicional nos encontraremos con el segundo teorema de incompletud para la teoría de conjuntos.

A partir de ahora, por teoría de conjuntos (TC) entendemos la teoría (dentro del lenguaje con la igualdad y con los dos parámetros $\forall$ y $\in$) que es el conjunto de consecuencias de los axiomas teórico-conjuntistas con los que el lector se sienta más cómodo. (Los axiomas estándar de Zermelo-Fraenkel funcionan bastante bien, si es que el lector no tiene otra preferencia; lo único que se pide es que el conjunto de axiomas sea recursivo y que sea lo suficientemente fuerte como para dar cuenta de las propiedades que comúnmente asociamos a los conjuntos.) Necesitamos dar una interpretación π de $\text{Cn}A_E$ dentro de TC. (Supondremos, en lo que queda de esta sección, que el lector está familiarizado con la sección 7 del capítulo II.) Sin embargo, la existencia de dicha π es un resultado común de la teoría de conjuntos, aunque no suele expresarse en estos términos. Necesitamos fórmulas del lenguaje de TC que expresen adecuadamente las ideas de ser un número natural, de ser la suma de dos números, etc. Para encontrar estas fórmulas, hay que ver cómo se puede "insertar" la aritmética de los números naturales en la teoría de conjuntos. Por un lado tenemos que los números naturales, como 2 o 7, no *parecen* ser conjuntos; sin embargo, al elegir, podemos seleccionar conjuntos que *representen* los números. La forma estándar de hacerlo es asociando

al 0 el conjunto $\emptyset$ y a $n+1$ el conjunto $n;n$ (es decir, $n \cup \{n\}$). Esto tiene la ventaja de que cada número es el conjunto de todos los números más pequeños que él (por ejemplo, $3 \in 7$). Sea ω la colección de todos estos conjuntos (estos "conjuntos-números"); entonces ω es el conjunto que representa $\mathbb{N}$.

La fórmula $\pi_\forall$ es resultado de la eliminación del símbolo definido ω de la fórmula $v_1 \in \omega$. De manera similar, la fórmula π_0 se obtiene a partir de la fórmula teórico conjuntista $v_1 = \emptyset$, y la fórmula π_S se obtiene a partir de $v_2 = v_1 \cup \{v_1\}$. La fórmula $\pi_<$ simplemente es $v_1 \in v_2$. Para π_+ usamos la traducción al lenguaje de TC de:

Para cualquier f, si $f: \omega \times \omega \to \omega$ y para todas a y b en ω tenemos que $f(a,\emptyset) = a$ y $f(a, b \cup \{b\}) = f(a,b) \cup \{f(a,b)\}$, entonces $f(v_1, v_2) = v_3$.

(La forma de llevar a cabo la traducción se sugiere parcialmente en el capítulo cero.) Las fórmulas $\pi_.$ y π_E se obtienen de manera similar.

Para que dicha π sea una interpretación de Cn A_E en TC, es necesario que TC cumpla con cierto número (en total 17) de condiciones.

(i) $\exists v_1 \pi_\forall$ debe estar en TC. Esto ciertamente sucede, ya que en la teoría de conjuntos se puede probar que ω es no vacío.

(ii) Para cada uno de los cinco símbolos de función f del lenguaje de A_E, TC debe contener un enunciado que asegure que π_f define una función sobre el conjunto definido por $\pi_\forall$. (El enunciado exacto que se requiere se plantea en la definición de interpretación de la sección 7 del capítulo II.) Para el caso de 0, tenemos como resultado de TC que existe un único conjunto vacío que además pertenece a ω. El caso de **S** es bastante sencillo, ya que π_S define una operación unaria sobre el universo de todos los conjuntos y ω es cerrado bajo esta operación. Para + hay que usar el teorema de recursión sobre ω. Esto es, podemos probar en TC (como se sugirió en la sección 4 del capítulo I) que existe una única $f: \omega \times \omega \to \omega$ tal que $f(a,\emptyset) = a$ y $f(a, b \cup \{b\}) = f(a,b) \cup \{f(a,b)\}$ para todas las a y b en ω. A

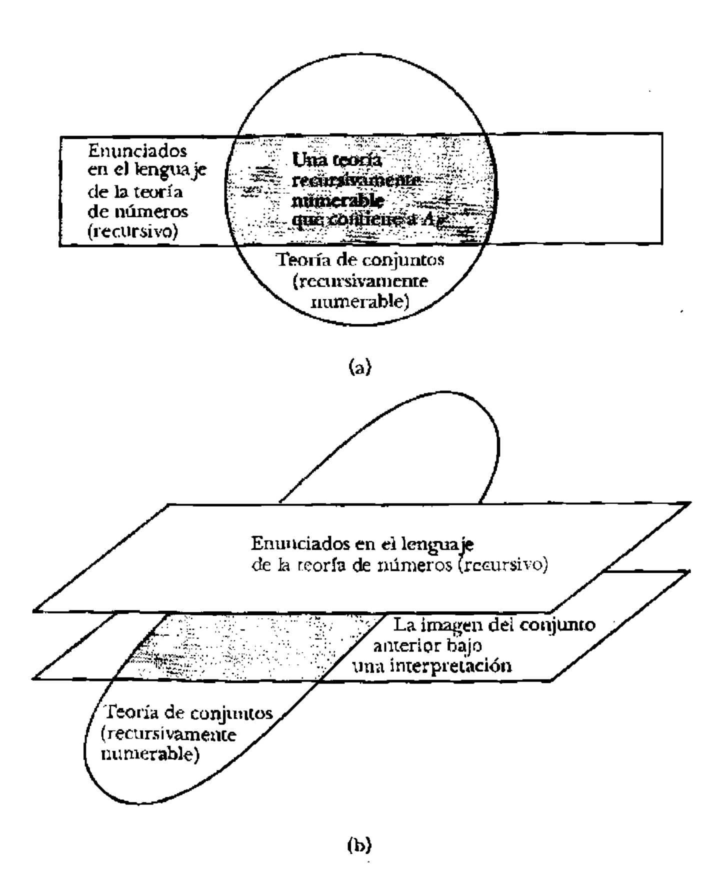


FIGURA 14. *Teoría de conjuntos y teoría de números. (a) Una imagen plana. (b) Una imagen más precisa.*

partir de esto queda claro qué propiedades debe tener π_+. Los casos de $\cdot$ y **E** requieren argumentos similares.

(iii) Para cada uno de los 11 enunciados σ de A_E, el enunciado σ^π debe estar en TC. Por ejemplo, para el caso de L3, tenemos en TC que para cualesquiera m y n en ω, o bien $m \in n$, o bien $m = n$, o bien $n \in m$.

Puesto que se trata de un número finito de condiciones, existe $\Phi \subseteq$ TC, donde Φ es finito, tal que π también es una interpretación de Cn A_E en Cn Φ.

Teorema 37D (Indecidibilidad fuerte de la teoría de conjuntos) Sea T una teoría del lenguaje de la teoría de conjuntos tal que $T \cup$ TC (o al menos $T \cup \Phi$) es consistente. Entonces $\sharp T$ no es recursivo.

Demostración Sea Δ la teoría consistente Cn $(T \cup \Phi)$. Sea Δ_0 la correspondiente teoría $\pi^{-1}[\Delta]$ en el lenguaje de la teoría de números. Por la sección 7 del capítulo II sabemos que Δ_0 es una teoría consistente (ya que Δ lo es). También tenemos que $A_E \subseteq \Delta_0$, pues si $\sigma \in A_E$, entonces $\sigma^\pi \in$ Cn $\Phi \subseteq \Delta$. De modo que, por la indecidibilidad fuerte de Cn A_E (teorema 35C), $\sharp\Delta_0$ no es recursivo.

Lo que tenemos que hacer ahora es derivar la no recursividad de T a partir de la no recursividad de Δ_0. Tenemos que

$$\sigma \in \Delta_0 \quad \text{sii} \quad \sigma^\pi \in \Delta$$

y, por el lema que presentaremos a continuación, $\sharp\sigma^\pi$ depende recursivamente de $\sharp\sigma$. Es decir, $\sharp\Delta_0 \leq_m \sharp\Delta$. Por lo tanto, $\sharp\Delta$ no puede ser recursivo, a menos que $\sharp\Delta_0$ lo sea. De manera similar tenemos que

$$\tau \in \Delta \quad \text{sii} \quad (\varphi \to \tau) \in T,$$

donde φ es la conjunción de los elementos de Φ. Dado que $\sharp(\varphi \to \tau)$ depende recursivamente de $\sharp\tau$, tenemos que $\sharp\Delta \leq_m \sharp T$ y, por lo tanto, $\sharp T$ no puede ser recursivo, a menos que $\sharp\Delta$ lo sea. ⊣

Lema 37E Existe una función recursiva p tal que, para toda fórmula α del lenguaje de la teoría de números, $p(\sharp\alpha) = \sharp(\alpha^{\pi})$.

Demostración En la sección 7 del capítulo II dimos una serie de instrucciones explícitas para construir α^{π}. En algunos casos, la construcción involucra fórmulas β^{π}, donde β es una fórmula más sencilla que α. Los métodos de las secciones 3 y 4 del capítulo III pueden aplicarse a los números de Gödel de tales fórmulas para demostrar que p es recursivo. Pero los detalles son bastante tediosos y los omitiremos. ⊣

Corolario 37F Si la teoría de conjuntos es consistente, entonces no es completa.

Demostración La teoría de conjuntos tiene un conjunto recursivo de axiomas, por lo que, si es completa, entonces es recursiva (por el inciso 21 de la sección 4 del capítulo III). Pero, por el último teorema, esto no puede ser si TC es consistente. ⊣

Corolario 37G En el lenguaje con igualdad y con un símbolo de predicado binario, el conjunto (de números de Gödel) de enunciados válidos no es recursivo.

Demostración parcial Dentro del contexto del teorema anterior, sea $T = \text{Cn}\,\emptyset$ el conjunto de los enunciados válidos. Entonces el teorema nos asegura que $\sharp T$ no es recursivo si suponemos que Φ es consistente. Todavía no hemos dado explícitamente el conjunto Φ, pero podemos asegurar al lector que es posible escoger Φ de modo que se pueda demostrar que es consistente. ⊣

Es importante observar que π *no* es una interpretación de $\text{Th}\,\mathfrak{N}$ en TC (a menos que TC sea inconsistente). Como consecuencia del lema 37E, tenemos que $\pi^{-1}[\text{TC}]$ es una teoría recursivamente numerable del lenguaje de $\mathfrak{N}$. Por lo tanto, no puede coincidir con $\text{Th}\,\mathfrak{N}$. Pero, además, contiene a la teoría completa $\text{Th}\,\mathfrak{N}$ sólo si es inconsistente.

Segundo teorema de incompletud de Gödel para la teoría de conjuntos

Podemos usar nuestros conocidos trucos para encontrar un enunciado σ de la teoría de números que indirectamente afirme que su propia interpretación σ^{π} no es un teorema de la teoría de conjuntos. Sea D la relación ternaria sobre $\mathbb{N}$ tal que

$\langle a, b, c\rangle \in D$ sii a es el número de Gödel de una fórmula α de la teoría de números y c es el número de Gödel de una deducción de $\alpha(\mathbf{S}^b\mathbf{O})^{\pi}$ a partir de los axiomas de TC.

La relación D es recursiva (por los argumentos típicos para estos casos); digamos que $\delta(v_1, v_2, v_3)$ representa D en $\mathrm{Cn}A_E$. Sea r el número de Gödel de

$$\forall v_3 \neg \delta(v_1, v_1, v_3)$$

y sea σ

$$\forall v_3 \neg \delta(\mathbf{S}^r\mathbf{0}, \mathbf{S}^r\mathbf{0}, v_3).$$

Observe que σ *dice* indirectamente que $\sigma^{\pi} \notin$ TC. A continuación demostraremos que dicha afirmación es correcta:

Lema 37H Si TC es consistente, entonces $\sigma^{\pi} \notin$ TC.

Demostración Supongamos lo contrario: que σ^{π} puede deducirse a partir de los axiomas de TC. Sea k el valor asignado por $\mathcal{G}$ a dicha deducción. Entonces, $\langle r, r, k\rangle \in D$.

$$\therefore\ A_E \vdash \delta(\mathbf{S}^r\mathbf{0}, \mathbf{S}^r\mathbf{0}, \mathbf{S}^k\mathbf{0});$$
$$\therefore\ A_E \vdash \exists v_3\, \delta(\mathbf{S}^r\mathbf{0}, \mathbf{S}^r\mathbf{0}, v_3);$$

es decir,

$$A_E \vdash \neg \sigma.$$

Usando nuestra interpretación π, concluimos que $\neg \sigma^{\pi}$ está en TC y, por lo tanto, TC es inconsistente. Así que

$$\text{TC es consistente} \Rightarrow \sigma^{\pi} \notin \text{TC}. \qquad \dashv$$

Esta prueba, como casi todas en este libro, se lleva a cabo en un contexto matemático informal; sin embargo, todo el trabajo de este libro podría haberse desarrollado dentro de TC. De hecho, se sabe que casi todo el trabajo en matemáticas puede llevarse a cabo en TC. Supongamos que lo hacemos así. Entonces, en lugar de demostrar un enunciado en español, tal como "TC es consistente $\Rightarrow$ $\sigma^{\pi} \notin$ TC", tendríamos una deducción, a partir de los axiomas de TC, de un enunciado en el lenguaje formal de la teoría de conjuntos:

$$(\text{Cons}\,(\text{TC}) \to \square).$$

En este caso, Cons (TC) es resultado de la traducción (adecuada) de "TC es consistente" al lenguaje de la teoría de conjuntos. De manera similar, $\square$ es el resultado de la traducción de "$\sigma^{\pi} \notin$ TC"; pero ya *tenemos* un enunciado en el lenguaje de la teoría de conjuntos que afirma que $\sigma^{\pi} \notin$ TC. Dicho enunciado no es sino σ^{π}. Esto claramente sugiere que $\square$ es σ^{π} (o algo equivalente a σ^{π} en TC), de donde obtenemos

$$(\text{Cons}\,(\text{TC}) \to \sigma^{\pi})$$

es un teorema de TC.

Ahora bien, *podemos* hacer las cosas de manera que $\square$ sea σ^{π}. En el párrafo anterior dimos un argumento que esperamos haya convencido al lector de que al menos esto es plausible. A partir de ello tendríamos el siguiente resultado:

Segundo teorema de incompletud de Gödel para la teoría de conjuntos El enunciado Cons (TC) no es un teorema de TC, a menos que TC sea inconsistente.

Demostración Por el argumento (de plausibilidad) antes dado,

$$(\text{Cons}\,(\text{TC}) \to \sigma^{\pi})$$

es un teorema de TC. De modo que si Cons (TC) es un teorema de TC, entonces σ^{π} también lo es. Pero, por el lema 37H, si $\sigma^{\pi} \in$ TC, entonces TC es inconsistente. $\dashv$

Por supuesto que si TC es inconsistente, entonces todo enunciado es teorema, incluido Cons (TC). Por esto, una demostración de Cons (TC) a partir de TC no podría convencer a nadie de la consistencia de TC. (En realidad, gracias al segundo teorema de Gödel se convencerían más bien de lo contrario.) Sin embargo, antes de tomar en cuenta el trabajo de Gödel, parecía natural esperar que Cons (TC) se pudiera demostrar a partir de hipótesis más débiles que los axiomas de la teoría de conjuntos, idealmente, hipótesis que ya se supiera que son consistentes. Ahora ya sabemos que Cons (TC) no pertenece a ninguna subteoría de TC, a menos que, por supuesto, TC sea inconsistente.

Nos quedamos con la conclusión de que toda teoría de conjuntos recursivamente axiomatizable (que cumpla con las condiciones de ser consistente y de ser lo suficientemente fuerte como para probar propiedades básicas de conjuntos) es una teoría incompleta. Esto plantea un nuevo desafío: encontrar axiomas para agregar a la teoría. Por un lado, quisiéramos tener nuevos axiomas para incrementar los alcances de la teoría. Por otro, quisiéramos que dichos axiomas reflejaran con claridad ideas intuitivas acerca de lo que verdaderamente son los conjuntos y de cómo se comportan.

Ejercicios

1. Sea σ un enunciado tal que

$$AP \vdash (\sigma \leftrightarrow \text{Dem}_{AP}\sigma).$$

   (De modo que σ dice "Soy demostrable", a diferencia del enunciado "Soy indemostrable" que mostró tener propiedades muy interesantes.) ¿Será que $AP \vdash \sigma$?

2. Sea T una teoría en un lenguaje recursivamente numerado y supongamos que hay una interpretación de $\text{Cn}\,A_E$ en T. Demuestre que T es fuertemente indecidible; es decir, que siempre que T' sea una teoría del lenguaje tal que $T \cup T'$ es consistente, entonces $\sharp T'$ no es recursivo.

8. *Representación de la exponenciación*[4]

En las secciones 1 y 2 de este capítulo estudiamos la teoría de ciertos reductos de $\mathfrak{N}$ y encontramos que eran decidibles. Después, en la sección 3 agregamos *tanto* el producto *como* la exponenciación y encontramos (en la sección 5) que la teoría que las incluía era indecidible. De hecho, hubiera sido suficiente agregar sólo el producto (y dejar de lado la exponenciación) para tener la indecidibilidad.

Sea $\mathfrak{N}_M$ el reducto de $\mathfrak{N}$ que se obtiene cuando se excluye la exponenciación:

$$\mathfrak{N}_M = (\mathbb{N}; 0, S, <, +, \cdot).$$

De modo que el símbolo **E** no aparece en el lenguaje de $\mathfrak{N}_M$. Sea A_M el subconjunto de A_E que no tiene ni a E1 ni a E2. El objetivo de esta sección es mostrar que todos los teoremas de las secciones 3 a la 5 de este capítulo siguen siendo válidos cuando "A_E" y "$\mathfrak{N}$" se sustituyen por "A_M" y "$\mathfrak{N}_M$", respectivamente. La clave para obtener este resultado está en demostrar que la exponenciación es representable en $\text{Cn}A_M$; es decir, hay una fórmula ε en el lenguaje de $\mathfrak{N}_M$ tal que para cualesquiera a y b,

$$A_M \vdash \forall z[\varepsilon(\mathbf{S}^a\mathbf{0}, \mathbf{S}^b\mathbf{0}, z) \leftrightarrow z = \mathbf{S}^{(a^b)}\mathbf{0}].$$

Así que $\varepsilon(x, y, z)$ podría usarse como un disfraz para simular la fórmula $x\mathbf{E}y = z$ que nos permitiría evitar el uso del símbolo **E**.

Si comenzamos a buscar qué relaciones y funciones son representables en $\text{Cn}\,A_M$, encontraremos que todo lo que se demostró que es representable en $\text{Cn}\,A_E$ es representable (usando la misma prueba) en $\text{Cn}A_M$ (excepto la exponenciación). Es decir, tenemos el catálogo de la sección 3 de este capítulo hasta el inciso 7. Para tener más, necesitamos demostrar que la exponenciación misma es representable en $\text{Cn}A_M$.

Sabemos que la exponenciación se puede definir mediante las ecuaciones recursivas:

$$a^0 = 1$$
$$a^{b+1} = a^b \cdot a.$$

[4] Esta sección se puede omitir sin que se pierda continuidad en el texto.

Basándonos en la recursión primitiva (inciso 13 del catálogo de la sección 3 de este capítulo, junto con el ejercicio 8 de esa misma sección), podemos pensar en definir

$$E^*(a,b) = \text{la mínima } s \text{ tal que } [(s)_0 = 1 \text{ y para toda } i < b,\ (s)_{i+1} = (s)_i \cdot a].$$

De manera que $a^b = (E^*(a,b))_b$. Esto todavía no nos da una demostración de la representabilidad de la exponenciación, ya que falta demostrar que la función decodificadora $(a)_b$ es representable en $\mathrm{Cn}\, A_M$. Pero en realidad no necesitamos esa función decodificadora en específico (que correspondía a una forma particular de codificar sucesiones). Lo único que necesitamos es *cualquier* función δ que se comporte como una función decodificadora; es decir, que tenga las propiedades que se presentan en el siguiente lema.

Lema 38A Existe una función δ representable en $\mathrm{Cn}\, A_M$ tal que, para todas $n, a_0, \ldots, a_n$, existe una s para la cual $\delta(s,i) = a_i$ para toda $i \leq n$.

Una vez que hemos establecido este lema, podemos definir

$$E^{**}(a,b) = \text{la mínima } s \text{ tal que } [\delta(s,0) = 1 \text{ y para toda } i < b,\ \delta(s,i+1) = \delta(s,i) \cdot a].$$

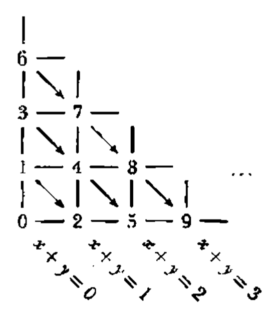
El lema nos garantiza que dicha s existe. Entonces, tanto E^{**} como la exponenciación son representables en $\mathrm{Cn}\, A_M$, ya que

$$a^b = \delta(E^{**}(a,b),b).$$

Gracias a algunos resultados de la teoría de números podremos obtener la función δ del lema anterior.

Una función de pareo

Lo primero que hay que hacer, para demostrar el lema, es construir una función para codificar y decodificar pares de números. Es bien sabido que existen funciones biyectivas de $\mathbb{N} \times \mathbb{N}$ sobre $\mathbb{N}$. En particular, tenemos la función J, donde $J(a,b)$ toma el valor escrito en el punto con coordenadas $\langle a,b \rangle$ del diagrama.



Por ejemplo, $J(2,1) = 8$ y $J(0,2) = 3$. Para obtener una ecuación que nos dé $J(a,b)$, basta observar que en la línea diagonal $x + y = n$ hay $n + 1$ puntos (con coordenadas en $\mathbb{N}$). De modo que

$J(a,b) =$ el número de puntos del plano a los cuales J asigna valores más pequeños

$=$ [el número de puntos en las líneas $x + y = n$ para $n = 0, 1, \ldots, (a + b - 1)$] + [el número de puntos de la línea $x + y = a + b$ para los cuales $x < a$]

$$= [1 + 2 + \cdots + (a + b)] + a$$

$$= \tfrac{1}{2}(a + b)(a + b + 1) + a$$

$$= \tfrac{1}{2}[(a + b)^2 + 3a + b].$$

Sean K y L las funciones proyectivas sobre los ejes, es decir, las únicas funciones tales que

$$K(J(a,b)) = a, \quad L(J(a,b)) = b.$$

Por ejemplo, $K(7) = 1$, la abscisa del punto $\langle 1, 2\rangle$ al que J asigna el número 7. De manera similar, $L(7) = 2$, la ordenada de dicho punto.

Afirmamos que J, K y L son representables en Cn A_M. La función

$$H(a) = \text{la mínima } b \text{ tal que } a \leq 2b$$

tiene la propiedad de que $H(a) = \frac{1}{2}a$, para toda a que sea par. Entonces podemos escribir

$$\begin{aligned} J(a,b) &= H((a+b)\cdot(a+b+1)) + a, \\ K(p) &= \text{la mínima } a \text{ tal que [para alguna } b \leq p, \\ &\quad J(a,b) = p], \\ L(p) &= \text{la mínima } b \text{ tal que [para alguna } a \leq p, \\ &\quad J(a,b) = p]. \end{aligned}$$

La forma en que estas últimas cuatro ecuaciones están dadas nos permite concluir que H, J, K y L son representables en $\text{Cn}A_M$.

La función β de Gödel

Sea β la función definida de la siguiente manera:

$$\begin{aligned} \beta(c,d,i) &= \text{el residuo de } c \div [1 + (i+1)\cdot d] \\ &= \text{la mínima } r \text{ tal que para alguna } q \leq c, \\ &\quad\; c = q\cdot[1+(i+1)\cdot d] + r. \end{aligned}$$

Esta extraña función sirve bastante bien como la función decodificadora para el lema 38A. Sea

$$\delta(s,i) = \beta(K(s), L(s), i).$$

Está claro que δ es representable en $\text{Cn}A_M$. Lo que no parece tan obvio es que dicha función satisfaga las condiciones del lema 38A. Queremos demostrar que:

> Para toda n y para cualesquiera $a_0, \ldots, a_n$, existen números c y d tales que, para toda $i \leq n$, $\beta(c,d,i) = a_i$. (*)

De donde se sigue que $\delta(J(c,d),i) = \beta(c,d,i) = a_i$ para toda $i \leq n$.

Ahora bien, (*) es una afirmación que pertenece a la teoría de números, no a la lógica. La demostración de (*) se basa en el teorema chino del residuo. Se dice que los números $d_0, \ldots, d_n$ son *primos relativos dos a dos* sii para cualesquiera d_i y d_j, con $i \neq j$, no hay un primo que los divida a ambos.

Teorema chino del residuo Sean $d_0, \ldots, d_n$ primos relativos dos a dos. Sean $a_0, \ldots, a_n$ números naturales tales que $a_i < d_i$. Entonces podemos encontrar un número c tal que, para toda $i \leq n$,

$$a_i = \text{el residuo de } c \div d_i.$$

Demostración Sea $p = \Pi_{i \leq n} d_i$, y dada cualquier c, sea $F(c)$ igual a la $(n+1)$-ada de residuos que se obtienen al dividir c entre $d_0, \ldots, d_n$. Obsérvese que hay p posibles valores para esa $(n+1)$-ada.

Afirmamos que F es inyectiva cuando se restringe al conjunto $\{k \mid 0 \leq k < p\}$, pues supongamos que $F(c_1) = F(c_2)$, entonces toda d_i divide a $|c_1 - c_2|$. Como las d_i son primos relativos dos a dos, entonces p debe dividir a $|c_1 - c_2|$. Pero esto implica, para c_1 y c_2 menores que p, que $c_1 = c_2$.

De modo que la restricción de F a $\{k \mid 0 \leq k < p\}$ toma todos los p posibles valores. En particular, toma (en algún punto c) el valor $\langle a_0, \ldots, a_n \rangle$. Y ése es justamente el número c que buscábamos. ⊣

Lema 38B Dada cualquier $s \geq 0$, los $s + 1$ números

$$1 + 1 \cdot s!,\ 1 + 2 \cdot s!,\ \ldots,\ 1 + (s+1) \cdot s!$$

son primos relativos dos a dos.

Demostración Todos estos números tienen la propiedad de que ningún factor primo q divide a $s!$, de modo que $q > s$. Si el primo q divide tanto a $1 + j \cdot s!$ como a $1 + k \cdot s!$, entonces divide a la diferencia, $|j - k| \cdot s!$. Como q no divide a $s!$, entonces divide a $|j - k|$. Pero como $|j-k| \leq s < q$, lo anterior sólo sucede si $|j-k| = 0$. ⊣

Demostración de (*) Supongamos que se nos dan $a_0, \ldots, a_n$. Necesitamos dos números c y d tales que, cuando c se divide entre $1 + (i+1) \cdot d$, el residuo es a_i, para $i \leq n$.

Sea s el máximo de $\{n, a_0, \ldots, a_n\}$ y tomemos $d = s!$. Entonces, por el lema 38B, los números $1 + (i+1) \cdot d$

son primos relativos dos a dos, para $i \leq n$. De modo que, por el teorema chino del residuo, hay una c tal que el residuo de $c \div [1 + (i + 1) \cdot d]$ es a_i para $i \leq n$. ⊣

Esto completa la demostración del lema 38A. Y por el argumento que se expuso después de enunciar ese lema, podemos concluir lo siguiente:

Teorema 38C La exponenciación es representable en $\mathrm{Cn}\, A_M$.

Una vez dotados con este teorema podemos regresar al inciso 7 de la sección 3 de este capítulo. La demostración que ahí se da establece ahora que la función en cuestión (cuyo valor en n es p_n) es representable en $\mathrm{Cn}A_M$, ya que dicha función se formó legítimamente a partir de relaciones y funciones (incluida la exponenciación) representables en $\mathrm{Cn}\, A_M$.

Lo mismo se observa a lo largo de las secciones 3 y 4. Las pruebas de representabilidad dadas en esas secciones establecen ahora la representabilidad en $\mathrm{Cn}A_M$. De manera que toda relación recursiva es representable en $\mathrm{Cn}A_M$. En caso de que la relación sea una función, entonces tenemos, además, que es funcionalmente representable. Las demostraciones dadas en la sección 5 de este capítulo se aplican a $\mathfrak{N}_M$ y A_M, así como a $\mathfrak{N}$ y A_E. En particular, tenemos la indecidibilidad fuerte de $\mathrm{Cn}A_M$: toda teoría T en el lenguaje de $\mathfrak{N}_M$, tal que $T \cup A_M$ sea consistente, no puede ser recursiva.

Obsérvese que toda relación definible en $\mathfrak{N}$ (es decir, cualquier relación aritmética) también es definible en $\mathfrak{N}_M$. En el caso particular de la exponenciación, dado que es representable en una subteoría de $\mathrm{Th}\,\mathfrak{N}_M$, tenemos que *forzosamente* es definible en $\mathfrak{N}_M$. Gracias a la nueva versión del teorema de Tarski, $\sharp\mathrm{Th}\,\mathfrak{N}_M$ no es definible en $\mathfrak{N}_M$ y, por lo tanto, $\sharp\mathrm{Th}\,\mathfrak{N}_M$ no puede ser aritmético.

Usando la terminología de la sección 7 del capítulo II, podemos decir que existe una interpretación fiel de $\mathrm{Th}\,\mathfrak{N}$ en $\mathrm{Th}\,\mathfrak{N}_M$. Se trata de la misma interpretación de todos los parámetros, excepto E, al que asigna una fórmula que define la exponenciación en $\mathfrak{N}_M$.

En la tabla X se resumen algunos de los resultados del capítulo III sobre la teoría de números y sus reductos.

Tabla X

Estructura	Teoría	Modelos de la teoría	Conjuntos definibles	Comentarios
$(\mathbb{N})$	Decidible. No finitamente axiomatizable. Admite eliminación de cuantificadores.	Cualquier conjunto infinito.	$\emptyset$ y $\mathbb{N}$. $\{0\}$ no es definible.	
$(\mathbb{N}; 0)$	Como el caso anterior.	Cualquier conjunto infinito con un elemento distinguido.	$\emptyset$, $\{0\}$, $\mathbb{N} - \{0\}$, $\mathbb{N}$. S no es definible.	
$(\mathbb{N}; 0, S)$	Como los casos anteriores.	Una parte estándar más cualquier cantidad de Z-cadenas.	Conjuntos finitos y cofinitos. $<$ no es definible.	$\{0\}$ es definible en $(\mathbb{N}; S)$.
$(\mathbb{N}; 0, S, <)$	Decidible. Finitamente axiomatizable. Admite eliminación de cuantificadores.	Como en el caso anterior, con cualquier orden entre las Z-cadenas.	Conjuntos finitos y cofinitos. $+$ no es definible.	$\{0\}$ y S son definibles en $(\mathbb{N}; <)$.
$(\mathbb{N}; 0, S, <, +)$	Decidible (Presburger).	Hay un orden denso entre las Z-cadenas sin máximo ni mínimo. Además, hay una operación adecuada de suma.	Conjuntos finalmente periódicos. $\cdot$ no es definible.	$\{0\}$, S y $<$ son definibles en $(\mathbb{N}; +)$.
$(\mathbb{N}; 0, S, <, +, \cdot)$	No es aritmética. $\therefore$ no es recursivamente axiomatizable.	Como en el caso anterior, pero con una operación de multiplicación adecuada.	Todas las relaciones aritméticas son definibles.	Las relaciones aritméticas son definibles en $(\mathbb{N}; S, \cdot)$, $(\mathbb{N}; +, \cdot)$ y $(\mathbb{N}; <, D)$, con $D(x, y) = (x)_y$.

Ejercicios

1. Sea $D(a, b) = (a)_b$. Muestre que toda relación aritmética es definible en la estructura $(\mathbb{N}; <, D)$. *Observación:* podríamos preguntarnos por qué $\text{Th}\,\mathfrak{N}_A$, la aritmética con la suma, es decidible (como se demostró en la sección 2 de este capítulo), mientras que $\text{Th}\,\mathfrak{N}_M$, la teoría de la aritmética con la suma y el producto, es indecidible. Una respuesta es que, como se demostró en esta sección, el producto nos permite codificar y decodificar sucesiones. El objetivo de este ejercicio es mostrar que una vez que se tiene una función decodificadora D y el orden, se tiene toda la complejidad de la aritmética con la suma, el producto y la exponenciación.

2. Demuestre que la relación suma $\{\langle a, b, c\rangle \mid a + b = c\}$ es definible en la estructura $(\mathbb{N}; S, \cdot)$. *Sugerencia:* ¿En qué condiciones se satisface la ecuación $S(ac) \cdot S(bc) = S(c \cdot c \cdot S(ab))$?

3. (a) Muestre que $\text{Th}(\mathbb{Z}; +, \cdot)$ es fuertemente indecidible. (Véase el ejercicio 2 de la sección 7 de este capítulo.)

   (b) (Esta parte presupone conocimientos de álgebra.) Muestre que la teoría de anillos es indecidible y que la teoría de anillos conmutativos es indecidible.

IV

LÓGICA DE SEGUNDO ORDEN

1. *Lenguajes de segundo orden*

Si se permite la cuantificación sobre símbolos de predicado o de función, es posible obtener —aunque a cierto costo— lenguajes más ricos y con mayor capacidad de expresión que los lenguajes de primer orden, que hemos considerado hasta ahora. Por ejemplo,

$$\exists x (Px \rightarrow \forall x\, Px)$$

es una fórmula válida que tiene como parámetros $\forall$ y P. Pero ya que esta fórmula es verdadera independientemente de cómo se interprete P, entonces podríamos también decir que

$$\forall \boldsymbol{P} \exists x (Px \rightarrow \forall x\, Px)$$

es válida. (En cuyo caso se tendría $\forall$ como único parámetro, ya que $\boldsymbol{P}$ se está considerando como una variable de predicado.)

Supongamos entonces que, además de los símbolos que se introdujeron al principio de la sección 1 del capítulo II, tenemos los siguientes símbolos lógicos:

4. Variables de predicado: Para todo entero positivo n tenemos las variables de predicado n-ario

$$\boldsymbol{X}_1^n, \boldsymbol{X}_2^n, \ldots$$

5. Variables de función: Para todo entero positivo n, tenemos las variables de función n-aria

$$\boldsymbol{F}_1^n, \boldsymbol{F}_2^n, \ldots$$

Para evitar confusión, lo que considerábamos antes variables, $v_1, v_2, \ldots$, se llamarán ahora variables *individuales*. Los términos se definen, igual que antes, como las expresiones que se construyen a partir de los símbolos de constante y las variables individuales al aplicar los símbolos de función (tanto los parámetros de función, como las variables de función). Las fórmulas atómicas son, otra vez, expresiones $Pt_1 \cdots t_n$ tales que $t_1, \ldots, t_n$ son términos y P es un símbolo de predicado n-ario (parámetro o variable). La definición de fórmula se extiende mediante nuevas operaciones de construcción de fórmulas: si φ es una fórmula, entonces $\forall \boldsymbol{X}_i^n \varphi$ y $\forall \boldsymbol{F}_i^n \varphi$ también lo son. La noción de variable que aparece libre en φ se define exactamente como antes. Un enunciado es una fórmula σ en la que ninguna variable (individual, de predicado o de función) aparece libre.

Debe notarse que los papeles que desempeñan los parámetros de predicado y las variables de predicado libres son esencialmente los mismos. La estrecha relación que hay entre los símbolos de constante y las variables individuales libres también existe entre los parámetros de función y las variables de función libres.

Por una *estructura* seguiremos entendiendo una función sobre el conjunto de los parámetros que cumple con las condiciones dadas en la sección 2 del capítulo II. Desde luego, es necesario extender la noción de satisfacción de una manera natural. Ahora V será el conjunto de todas las variables, individuales, de predicado o de función. Sea s una función sobre V tal que a cada variable le asigna el objeto de tipo adecuado. Entonces $s(v_1)$ es un elemento del universo, $s(X^n)$ es una relación n-aria sobre el universo y $s(\boldsymbol{F}^n)$ es una operación n-aria. Para un término t, $\bar{s}(t)$ se define de la manera natural. En particular, si $\boldsymbol{F}$ es una variable de función, entonces $\bar{s}(\boldsymbol{F}t_1 \cdots t_n)$ es el resultado de aplicar la función $s(\boldsymbol{F})$ a $\langle \bar{s}(t_1), \ldots, \bar{s}(t_n) \rangle$. La satisfacción de fórmulas atómicas también se define esencialmente como antes. Si $\boldsymbol{X}$ es una variable de predicado,

$$\models_{\mathfrak{A}} \boldsymbol{X}t_1 \cdots t_n[s] \quad \text{sii} \quad \langle \bar{s}(t_1), \ldots, \bar{s}(t_n) \rangle \in s(\boldsymbol{X}).$$

Las únicas características nuevas de la definición de satisfacción provienen de nuestros nuevos cuantificadores.

5. $\models_{\mathfrak{A}} \forall X_i^n\ \varphi[s]$ sii para toda relación n-aria R sobre $|\mathfrak{A}|$, se tiene que $\models_{\mathfrak{A}} \varphi[s(X_i^n \mid R)]$.

6. $\models_{\mathfrak{A}} \forall F_i^n\ \varphi[s]$ sii para toda función $f : |\mathfrak{A}|^n \to |\mathfrak{A}|$, se tiene que $\models_{\mathfrak{A}} \varphi[s(F_i^n \mid f)]$.

Una vez más queda claro que los valores de s que realmente importan son los de las variables libres de la fórmula. Dado cualquier enunciado σ, podemos hablar sin ambigüedad de su verdad o falsedad en $\mathfrak{A}$. La implicación lógica (semántica) se define exactamente como antes.

EJEMPLO 1 Un buen orden es una relación de orden tal que, para todo conjunto no vacío, hay un elemento mínimo (con respecto al orden). Esta condición puede traducirse al siguiente enunciado de segundo orden:

$$\forall X(\exists y\, Xy \to \exists y(Xy \land \forall z(Xz \to y \leq z))).$$

Aquí, como en el resto del capítulo, omitimos los subíndices de X y F cuando son irrelevantes, y los superíndices cuando, por el contexto, queda claro cuáles son.

EJEMPLO 2 Uno de los postulados de Peano (el postulado de inducción) establece que todo conjunto de números naturales que tenga al 0 y que sea cerrado bajo la operación sucesor es, en realidad, el conjunto de todos los números naturales. Esto puede traducirse al lenguaje de segundo orden de la teoría de los números como sigue:

$$\forall X(X0 \land \forall y(Xy \to XSy) \to \forall y\, Xy).$$

Todo modelo de S1, S2 y del postulado de inducción de Peano anterior es isomorfo a $(\mathbb{N}; 0, S)$; véase el ejercicio 1. De modo que este conjunto de enunciados es categórico; es decir, todos sus modelos son isomorfos.

EJEMPLO 3 Si φ es una fórmula en la que la variable de predicado X^n no aparece libre, entonces la fórmula

$$\exists X^n\, \forall v_1 \cdots \forall v_n[X^n v_1 \cdots v_n \leftrightarrow \varphi]$$

es válida. (Es posible que, en la fórmula φ, haya otras variables libres además de $v_1, \ldots, v_n$). Esta nueva fórmula

nos dice que hay una relación que consiste exactamente en las n-adas que satisfacen φ. Los fórmulas de este tipo se conocen como *fórmulas de comprehensión relacionales*. También existen las *fórmulas de comprehensión funcionales* análogas. Si ψ es una fórmula en la que la variable $\boldsymbol{F}^n$ no aparece libre, entonces

$$\begin{aligned}&\forall v_1 \cdots \forall v_n \exists ! v_{n+1}\, \psi \rightarrow \\ &\quad \exists \boldsymbol{F}^n\, \forall v_1 \cdots \forall v_{n+1}(\boldsymbol{F}^n v_1 \cdots v_n = v_{n+1} \leftrightarrow \psi)\end{aligned}$$

es válida. ("$\exists ! v_{n+1}\psi$" es una abreviación de la fórmula obtenida en el ejercicio 21 de la sección 2 del capítulo II).

EJEMPLO 4 En el campo ordenado de los números reales, todo conjunto no vacío acotado tiene una mínima cota superior. Esto se puede traducir al siguiente enunciado de segundo orden:

$$\begin{aligned}&\forall X[\exists y\, \forall z(Xz \rightarrow z \leq y) \wedge \exists z\, Xz \rightarrow \\ &\quad \exists y\, \forall y'(\forall z(Xz \rightarrow z \leq y') \leftrightarrow y \leq y')].\end{aligned}$$

Se sabe, además, que todo campo ordenado que satisfaga este enunciado de segundo orden es isomorfo al campo ordenado de los reales.

EJEMPLO 5 Para toda $n \geq 2$, tenemos un enunciado de primer orden λ_n que es la traducción de "Hay al menos n cosas". Por ejemplo, λ_3 es

$$\exists x\, \exists y\, \exists z\, (x \neq y \wedge x \neq z \wedge y \neq z).$$

La clase de los modelos del conjunto $\{\lambda_2, \lambda_3, \ldots\}$ es una clase EC_Δ, compuesta por las estructuras infinitas. Hay *un único* enunciado de segundo orden tal que es equivalente. Un conjunto es infinito sii existe un orden sobre él que no tiene último elemento. De manera más sencilla: un conjunto es infinito sii existe una relación antirreflexiva y transitiva R sobre el conjunto cuyo dominio es

todo el conjunto. Esta condición puede traducirse a un enunciado de segundo orden λ_∞:

$$\exists X[\forall u \forall v \forall w (Xuv \to Xvw \to Xuw) \wedge \forall u \neg Xuu \wedge \forall u \exists v X uv].$$

Otro enunciado que define (usando una variable de función) la clase de las estructuras infinitas es

$$\exists F[\forall x \forall y (Fx = Fy \to x = y) \wedge \exists z \forall x Fx \neq z],$$

el cual afirma que existe una función inyectiva que no es suprayectiva.

El ejemplo anterior muestra que el teorema de compacidad no se cumple para la lógica de segundo orden:

Teorema 41A Existe un conjunto insatisfactible de enunciados de segundo orden tal que todos sus subconjuntos finitos son satisfactibles.

Demostración Utilizando la notación del ejemplo anterior, el conjunto es

$$\{\neg \lambda_\infty, \lambda_2, \lambda_3, \ldots\}. \qquad \dashv$$

El teorema de Löwenheim-Skolem también falla para la lógica de segundo orden. Cuando hablamos del *lenguaje de la igualdad*, nos referimos al lenguaje (con $=$) que tiene a $\forall$ como único parámetro. Una estructura de este lenguaje puede concebirse simplemente como un conjunto no vacío. En particular, una estructura así está determinada, salvo isomorfismo, por su cardinalidad. Por lo tanto, un enunciado de este lenguaje está determinado, salvo equivalencia lógica, por el conjunto de las cardinalidades de sus modelos (conocido como su *espectro*).

Teorema 41B Existe un enunciado del lenguaje de segundo orden de la igualdad que es verdadero en un conjunto sii su cardinalidad es $2^{\aleph_0}$.

Demostración, usando conceptos de álgebra y análisis Consideremos primero la conjunción de axiomas (de primer orden) de un campo ordenado y agreguemos después el enunciado de segundo orden que establece la propiedad de la

mínima cota superior (véase el ejemplo 4 de esta sección). Éste es un enunciado cuyos modelos son exactamente los isomorfos al campo ordenado real (es decir, las estructuras isomorfas al campo ordenado de los números reales). Convertiremos ahora los parámetros 0, 1, $+$, $\cdot$ y $<$ en variables (individuales, de función o de predicado, según sea el caso) que se cuantificarán existencialmente. El enunciado que resulta tiene las propiedades deseadas. ⊣

Existen otros números cardinales que, como el caso que acabamos de ver, caracterizan aspectos de la lógica de segundo orden. Véase el ejercicio 2.

Teorema 41C El conjunto de los números de Gödel de los enunciados válidos de segundo orden no es definible en $\mathfrak{N}$ mediante una fórmula de segundo orden.

En este caso estamos suponiendo, desde luego, que la forma en que se asignaron los números de Gödel a las expresiones de segundo orden es similar a la que se usó antes. Aunque la prueba que presentaremos aquí se refiere al lenguaje de segundo orden de la teoría de números, el teorema es válido para cualquier lenguaje recursivamente numerado que tenga al menos un símbolo de predicado binario.

Demostración Sea T^2 la teoría de segundo orden de $\mathfrak{N}$; es decir, el conjunto de enunciados de segundo orden verdaderos en $\mathfrak{N}$. El argumento que se usó para probar el teorema de Tarski muestra también que $\sharp T^2$ no se puede definir en $\mathfrak{N}$ mediante una fórmula de segundo orden.

Sea α la conjunción de los elementos de A_E junto con el postulado de inducción de segundo orden de Peano (Ejemplo 2). Todo modelo de α es isomorfo a $\mathfrak{N}$; véase el ejercicio 1. De modo que, para todo enunciado σ,

$$\sigma \in T^2 \quad \text{sii} \quad (\alpha \to \sigma) \text{ es válida.}$$

Por lo tanto, el conjunto de (los números de Gödel de) los enunciados válidos no es definible, pues de otro modo $\sharp T^2$ tendría que serlo. ⊣

Por fuerza, el conjunto de números de Gödel de los enunciados válidos no es aritmético, ni tampoco recursivamente numerable. Lo que quiere decir que el teorema de numerabilidad falla para la lógica de segundo orden. (Con respecto al primer resultado, podemos agregar que es posible demostrar que este conjunto tampoco es definible en la teoría de números de orden tres, ni siquiera en la de orden ω; sin embargo, éstos son temas que aquí dejaremos de lado.)

Resulta interesante comparar un enunciado universal de segundo orden, como el postulado de inducción de Peano

$$\forall X(X0 \wedge \forall y\,(Xy \rightarrow XSy) \rightarrow \forall y\, Xy),$$

con el "esquema" de primer orden correspondiente; es decir, con el conjunto de enunciados

$$\varphi(0) \wedge \forall y\,(\varphi(y) \rightarrow \varphi(Sy)) \rightarrow \forall y\, \varphi(y),$$

donde φ es una fórmula de primer orden que sólo tiene a v_1 libre. Si $\mathfrak{A}$ es un modelo del postulado de inducción de Peano, entonces cualquier subconjunto de $|\mathfrak{A}|$ que contenga a $0^{\mathfrak{A}}$ y sea cerrado bajo $S^{\mathfrak{A}}$ es en realidad todo $|\mathfrak{A}|$. Por otro lado, si $\mathfrak{A}$ es un modelo del esquema de axioma correspondiente, lo único que podemos decir es que todo subconjunto *definible* de $\mathfrak{A}$ que contenga a $0^{\mathfrak{A}}$ y sea cerrado bajo $S^{\mathfrak{A}}$ es todo $|\mathfrak{A}|$. Es posible que haya subconjuntos indefinibles en los que esto no se cumpla. (Por ejemplo, tómese cualquier modelo $\mathfrak{A}$ de $\text{Th}(\mathbb{N}; 0, S)$ que tenga Z-cadenas. En este caso, $\mathfrak{A}$ satisface el esquema de axioma en cuestión, pero no satisface el postulado de segundo orden de inducción. El conjunto de puntos estándar simplemente no es definible en $\mathfrak{A}$.)

Ejercicios

1. Muestre que toda estructura del lenguaje con los parámetros $\forall$, 0 y S, que satisfaga los enunciados

$$\forall x\, Sx \neq 0 \qquad \text{(S1)}$$

$$\forall x \forall y(Sx = Sy \rightarrow x = y) \qquad \text{(S2)}$$

y el postulado de inducción de Peano

$$\forall X(X0 \wedge \forall y(Xy \to XSy) \to \forall y Xy)$$

es isomorfo a $\mathfrak{N}_S = (\mathbb{N}; 0, S)$.

2. (a) Formule un enunciado del lenguaje de segundo orden de la igualdad, que sea verdadero en un conjunto sii su cardinalidad es $\aleph_0$.
   (b) Haga lo mismo para $\aleph_1$.

3. Sea φ una fórmula en la que únicamente la variable de predicado n-ario X aparece libre. Digamos que una relación n-aria R sobre $|\mathfrak{A}|$ está *implícitamente definida* en $\mathfrak{A}$ por φ sii $\mathfrak{A}$ satisface φ con una asignación de R a X, pero no satisface φ con ninguna otra asignación de otra relación a X. Muestre que $\sharp\mathrm{Th}\,\mathfrak{N}$, el conjunto de los números de Gödel de los enunciados de primer orden verdaderos en $\mathfrak{N}$, está implícitamente definido en $\mathfrak{N}$ por una fórmula sin variables de predicado o de función cuantificadas. *Sugerencia*: La idea es plantear las condiciones que el conjunto de enunciados verdaderos debe cumplir.

4. Considere un lenguaje (con igualdad) que tiene los símbolos de predicado unarios I, S y el símbolo de predicado binario E. Encuentre un enunciado de segundo orden σ tal que (i) si A es un conjunto para el que $A \cap \mathcal{P}A = \emptyset$ y si $|\mathfrak{A}| = A \cup \mathcal{P}A$, $I^{\mathfrak{A}} = A$, $S^{\mathfrak{A}} = \mathcal{P}A$, $E^{\mathfrak{A}} = \{\langle a,b\rangle \mid a \in b \subseteq A\}$, entonces $\mathfrak{A}$ es un modelo de σ; y (ii) todo modelo de σ es isomorfo a uno del tipo descrito en (i). *Observación:* En términos intuitivos, σ es la traducción de "$S = \mathcal{P}I$".

2. *Funciones de Skolem*

Queremos mostrar cómo, dada una fórmula de *primer* orden, es posible encontrar una fórmula prenex de segundo orden lógicamente equivalente, con la siguiente estructura:

cuantificadores existenciales	cuantificadores individuales universales	fórmula sin cuantificadores

Ésta es una fórmula prenex en la que todos los cuantificadores universales son individuales y se encuentran después de una serie de cuantificadores existenciales individuales y de función.

Si consideramos el ejemplo más sencillo, observamos que:

$$\forall x \exists y\, \varphi(x,y) \models\!\!\!\dashv \exists \boldsymbol{F} \forall x\, \varphi(x,\boldsymbol{F}x).$$

Es fácil ver por qué se cumple en la dirección "$\dashv$". Para la otra dirección, "$\models$", consideremos una estructura $\mathfrak{A}$ y una función de asignación s que satisfaga $\forall x \exists y\, \varphi(x, y)$. Nosotros sabemos que para toda $a \in |\mathfrak{A}|$ existe al menos una $b \in |\mathfrak{A}|$ tal que:

$$\models_{\mathfrak{A}} \varphi(x,y)\, [s\,(x \mid a)(y \mid b)].$$

Si para cada a elegimos una de esas b (utilizando el axioma de elección), entonces tenemos una función f sobre $|\mathfrak{A}|$ dada por $f(a) = b$. De modo que:

$$\models_{\mathfrak{A}} \forall x\, \varphi(x, \boldsymbol{F}x)[s\,(\boldsymbol{F} \mid f)].$$

Esta función f se conoce como una *función de Skolem* para la fórmula $\forall x \exists y\, \varphi$ en la estructura $\mathfrak{A}$.

El mismo argumento se aplica de manera más general. Como segundo ejemplo, supongamos que comenzamos con la fórmula

$$\exists y_1 \forall x_1 \exists y_2 \forall x_2 \forall x_3 \exists y_3\, \psi(y_1, y_2, y_3).$$

(Hemos listado únicamente y_1, y_2 y y_3, pero también es posible que haya otras variables libres en ψ.) En este caso ya se tiene el cuantificador existencial $\exists y_1$ a la izquierda. Lo que queda es

$$\forall x_1 \exists y_2 \forall x_2 \forall x_3 \exists y_3\, \psi(y_1, y_2, y_3).$$

Éste es un caso especial del primer ejemplo (con $\varphi(x_1,y_2) = \forall x_2\; \forall x_3\; \exists y_3\; \psi(y_1,y_2,y_3)$). Esto es, como antes, lógicamente equivalente a

$$\exists \boldsymbol{F}_2 \forall x_1 \forall x_2 \forall x_3 \exists y_3\, \psi(y_1, \boldsymbol{F}_2\, x_1, y_3).$$

Ahora ya tenemos los cuantificadores existenciales $\exists y_1 \; \exists F_2$ a la izquierda; lo que queda es

$$\forall x_1 \; \forall x_2 \; \forall x_3 \; \exists y_3 \; \psi(y_1, F_2 x_1, y_3).$$

Usando el mismo razonamiento que antes, esto es lógicamente equivalente a:

$$\exists F_3 \; \forall x_1 \; \forall x_2 \; \forall x_3 \; \psi(y_1, F_2 x_1, F_3 x_1 x_2 x_3),$$

donde F_3 es una variable de función ternaria. De modo que la fórmula original es equivalente a:

$$\exists y_1 \; \exists F_2 \; \exists F_3 \; \forall x_1 \; \forall x_2 \; \forall x_3 \; \psi(y_1, F_2 x_1, F_3 x_1 x_2 x_3).$$

Si ψ no tiene cuantificadores, entonces está en la forma buscada.

Teorema de la forma normal de Skolem Dada cualquier fórmula de primer orden, es posible encontrar una fórmula de segundo orden lógicamente equivalente que esté formada por:

(a) Primero una serie (que puede ser vacía) de cuantificadores existenciales individuales y de función, seguida de

(b) Una serie (que puede ser vacía) de cuantificadores individuales universales, seguida de

(c) Una fórmula sin cuantificadores.

Se puede hacer una demostración formal usando inducción, pero el ejemplo anterior muestra el método general.

Recuérdese que una fórmula universal ($\forall_1$) es una fórmula prenex de primer orden cuyos cuantificadores son todos universales: $\forall x_1 \; \forall x_2 \cdots \forall x_k \; \alpha$, donde α carece de cuantificadores. De manera similar, una fórmula existencial ($\exists_1$) es una fórmula prenex de primer orden cuyos cuantificadores son todos existenciales.

Corolario 42A Dada cualquier fórmula de primer orden φ, es posible encontrar una fórmula universal θ en un lenguaje extendido con símbolos de función, tal que φ es satisfactible sii θ es satisfactible.

Si aplicamos este corolario a $\neg\varphi$, obtenemos una fórmula existencial (con símbolos de función) que es válida sii φ es válida.

Demostración Una vez más, sólo ilustraremos la situación mediante un ejemplo. Supongamos que φ es

$$\exists y_1 \forall x_1 \exists y_2 \forall x_2 \forall x_3 \exists y_3\, \psi(y_1, y_2, y_3).$$

Lo primero es sustituir φ por la fórmula lógicamente equivalente en la forma de Skolem:

$$\exists y_1 \exists F_2 \exists F_3 \forall x_1 \forall x_2 \forall x_3\, \psi(y_1, F_2 x_1, F_3 x_1 x_2 x_3).$$

Entonces, como θ tomamos:

$$\forall x_1 \forall x_2 \forall x_3\, \psi(c, f x_1, g x_1 x_2 x_3),$$

donde c, f y g son nuevos símbolos de función que tienen cero, una y tres variables, respectivamente. En general, θ *no* es lógicamente equivalente a φ; sin embargo, lo que sí tenemos es que $\theta \models \varphi$ (en el lenguaje extendido). Y todo modelo $\mathfrak{A}$ de φ puede expandirse (definiendo adecuadamente $c^{\mathfrak{A}}, f^{\mathfrak{A}}$ y $g^{\mathfrak{A}}$) para que sea un modelo de θ. Por lo tanto, φ y θ son "igualmente satisfactibles". $\dashv$

Este resultado reduce el problema general de verificar la satisfactibilidad de las fórmulas de primer orden al caso particular de las fórmulas universales (con símbolos de función). De igual modo, el problema de la verificación de validez se reduce al caso $\exists_1$. A partir de estas reducciones podemos obtener un resultado de indecidibilidad para la lógica de primer orden:

Corolario 42B Considere un lenguaje recursivamente numerado con un símbolo de predicado binario y una infinidad de símbolos de función de k variables, para cada $k \geq 0$. Entonces:

(a) El conjunto de los números de Gödel de los enunciados universales (de primer orden) satisfactibles no es recursivo.

(b) El conjunto de los números de Gödel de los enunciados existenciales (de primer orden) válidos no es recursivo.

Demostración (b) Dado cualquier enunciado σ, y aplicando a $\neg\sigma$ el corolario 42A, podemos encontrar explícitamente un enunciado existencial que sea válido sii σ es válido. Por consiguiente, un procedimiento de decisión para los enunciados existenciales válidos daría un procedimiento de decisión para todos los enunciados válidos arbitrarios. Pero esto último contradiría el teorema de Church. $\dashv$

Se obtienen resultados análogos con variables de predicado en lugar de variables de función, aunque la demostración es más laboriosa. Supongamos que se empieza con una fórmula de primer orden. Ésta es equivalente a una fórmula ψ en la forma normal de Skolem; para simplificar, supongamos que $\psi = \exists \boldsymbol{F}\varphi$, donde φ es una fórmula que sólo tiene cuantificadores individuales y $\boldsymbol{F}$ es una variable de función unaria. Podemos elegir φ de tal manera que $\boldsymbol{F}$ ocurra únicamente en ecuaciones de la forma $u = \boldsymbol{F}t$ (donde t y u son términos que no contienen $\boldsymbol{F}$). Esto se puede hacer sustituyendo, por ejemplo, una fórmula atómica $\alpha(\boldsymbol{F}t)$ ya sea por $\forall x(x = \boldsymbol{F}t \rightarrow \alpha(x))$ o por $\exists x(x = \boldsymbol{F}t \wedge \alpha(x))$.

Lo siguiente es observar que una fórmula

$$\exists \boldsymbol{F}__u = \boldsymbol{F}t__,$$

donde $\boldsymbol{F}$ ocurre sólo en la forma mostrada, es equivalente a

$$\exists \boldsymbol{X}(\forall y\, \exists !z\, \boldsymbol{X}yz \wedge __\boldsymbol{X}tu__).$$

Si se sigue en esta dirección (cosa que no haremos aquí), se podrá ver que toda fórmula de primer orden es equivalente a una fórmula de segundo orden compuesta por:

(a) Una serie de cuantificadores existenciales de predicado, seguida de

(b) Una serie de cuantificadores individuales universales, seguida de

(c) Una serie de cuantificadores existenciales individuales, seguida de

(d) Una fórmula sin cuantificadores.

Existen también las versiones correspondientes de los corolarios 42A y 42B (véase el ejercicio 4). El análogo del corolario 42A reduce el problema de verificar la satisfactibilidad de una fórmula de primer orden al caso especial de fórmulas $\forall_2$ (con símbolos de predicado). El problema de verificar la validez se reduce, a su vez, al caso $\exists_2$.

El análogo del corolario 42B puede compararse con el ejercicio 10 de la sección 6 del capítulo II, donde se muestra que el conjunto de enunciados $\forall_2$ válidos sin símbolos de función es decidible.

Expansiones de Herbrand

Hemos visto (en el corolario 42A) cómo encontrar, dada una fórmula de la lógica de primer orden, una fórmula universal "igualmente satisfactible". De modo que (corolario 42B) el problema de la satisfactibilidad de fórmulas en la lógica de primer orden es *reducible* al de la satisfactibilidad de fórmulas universales.

Ahora daremos un paso más: la satisfactibilidad de estas fórmulas universales es reducible —aunque en un sentido más débil— a la satisfactibilidad en la lógica de *enunciados*.

EJEMPLO Sabemos que $\forall x \, \exists y \, Pxy \not\models \exists y \, \forall x \, Pxy$. Sin embargo supongamos que no lo sabemos y que queremos determinar si la implicación lógica se cumple o no. Esto es equivalente a determinar si la hipótesis $\forall x \, \exists y \, Pxy$, junto con la negación de la conclusión $\neg \exists y \, \forall x \, Pxy$ es insatisfactible o no.

Gracias al teorema de la forma normal de Skolem, podemos reemplazar estos enunciados por un tipo de enunciados lógicamente equivalentes: quisiéramos determinar si $\exists F \, \forall x \, PxFx$ junto con $\exists G \, \forall y \, \neg PGyy$ es insatisfactible o no. De la misma manera que en el corolario 42A, sustituimos estos enunciados por enunciados

universales igualmente satisfactibles; deseamos determinar si el conjunto $\{\forall x\, Pxfx,\ \forall y\, \neg Pgyy\}$ es insatisfactible o no (aquí f y g son nuevos símbolos de función).

Ahora bien, este conjunto de enunciados universales *sí* es satisfactible, e incluso se puede hacer que genere su propio modelo. Aquí mostraremos cómo hacerlo. Para el universo de nuestro modelo tomaremos el *universo H de Herbrand*, que es el conjunto de todos los términos (en el lenguaje con f y g). De modo que H contiene, para cualquier variable u, los términos

$$u,\ fu,\ gu,\ ffu,\ fgu, \ldots$$

Sea Δ el conjunto de todas las *instancias* de los enunciados universales en cuestión; esto es, las fórmulas que se obtienen cuando se quitan los cuantificadores universales y se insertan (en las variables universalmente cuantificadas) términos arbitrarios del universo de Herbrand. Entonces Δ contiene, para cualquier variable u, las fórmulas sin cuantificadores

$$Pufu,\ Pgufgu, \ldots,\ \neg Pguu,\ \neg Pgfufu, \ldots$$

Examinemos ahora Δ desde el punto de vista de la lógica de *enunciados*. Los símbolos de enunciado son las fórmulas atómicas, por ejemplo, $Pgfufu$. En nuestro ejemplo, Δ es satisfactible en la lógica de enunciados. Es decir, hay una asignación de verdad v sobre el conjunto de símbolos de enunciado tal que $\overline{v}(\alpha) = V$, para toda α en Δ. A continuación damos una v que cumple con eso:

$$v(Pt_1t_2) = \begin{cases} V & \text{si } t_1 \text{ es más corto que } t_2 \\ F & \text{si } t_1 \text{ es al menos tan largo como } t_2 \end{cases}$$

Por último, utilizaremos esta asignación de verdad v (en la lógica de enunciados) para dar una estructura $\mathfrak{H}$ (en lógica de primer orden) que será un modelo de los enunciados universales. El universo es el universo de Herbrand: $|\mathfrak{H}| = H$. (Este argumento tiene muchos elementos en común con la prueba de completud de la

sección 5 del capítulo II.) Los símbolos de función se interpretan de manera autónoma –como si se nombraran a sí mismos–: $f^{\mathfrak{H}}(t)$ es ft y $g^{\mathfrak{H}}(t)$ es gt. v nos sirve para interpretar el símbolo de predicado P:

$$\langle t_1, t_2 \rangle \in P^{\mathfrak{H}} \Longleftrightarrow v(Pt_1t_2) = V$$

Esta estructura funciona. Primero, $\models_{\mathfrak{H}} \forall x\, Px\, fx$, ya que para cualquier término t del universo de Herbrand, $\langle t, ft \rangle \in P^{\mathfrak{H}}$. Segundo, $\models_{\mathfrak{H}} \forall y\, \neg Pgy\, y$, pues para todo término t del universo de Herbrand, $\langle gt, t \rangle \notin P^{\mathfrak{H}}$.

Concluimos que la hipótesis $\forall x\, \exists y\, Pxy$ junto con la negación de la conclusión $\neg \exists y\, \forall x\, Pxy$ es satisfactible, y por lo tanto $\forall x\, \exists y\, Pxy \not\models \exists y\, \forall x\, Pxy$.

¿Hasta qué punto podemos hacer una generalización a partir de este ejemplo? Supongamos, para hacerlo más sencillo, que el lenguaje no contiene a la igualdad. (El ejercicio 7 muestra cuáles son las modificaciones que hay que hacer para integrar la igualdad.) Supongamos que queremos determinar si $\Gamma \models \varphi$ o no, para un conjunto de fórmulas de la lógica de primer orden $\Gamma; \varphi$. Esto equivale a determinar si el conjunto $\Gamma; \neg\varphi$ es insatisfactible o no.

Podemos reemplazar cada una de estas fórmulas por una fórmula lógicamente equivalente en la forma normal de Skolem. Luego, tal como en el corolario 42A, obtenemos un conjunto Ψ de fórmulas universales, igualmente satisfactible. (Al aplicar la forma normal de Skolem, se usan *diferentes* símbolos de función de Skolem para cada una de las fórmulas, de modo que no hay posibilidad de que las fórmulas resultantes se contradigan.) Esto nos conduce a la siguiente situación:

$$\Gamma \models \varphi \Longleftrightarrow \Psi \text{ es insatisfactible,}$$

donde Ψ es un conjunto de fórmulas universales.

Sea H el universo de Herbrand; es decir, el conjunto de todos los términos del lenguaje de Ψ. Sea Δ el conjunto de todas las instancias de las fórmulas universales en Ψ (es decir, las fórmulas que se obtienen cuando se quitan los cuantificadores universales y se insertan, en lugar de las variables universalmente cuantificadas, términos arbitrarios del universo de Herbrand). Entonces Δ está compuesto solamente por fórmulas

sin cuantificadores. Consideremos Δ desde el punto de vista de la lógica de enunciados, donde los símbolos de enunciado son las fórmulas atómicas.

Caso I: Δ es insatisfactible en la lógica de enunciados. En este caso, podemos concluir que Ψ es insatisfactible y $\Gamma \models \varphi$ en la lógica de primer orden. Esto se debe a que una fórmula universal implica lógicamente a todas sus instancias. Por consiguiente, $\Psi \models \delta$ para toda δ en Δ (en lógica de primer orden). Todo modelo de Ψ debe ser modelo de Δ; pero de un modelo $\mathfrak{A}$ de Δ podemos obtener una asignación de verdad v que satisfaga Δ en la lógica de enunciados. (Recuérdese el ejercicio 3 de la sección 4 del capítulo II. Nótese la interesante conexión entre la lógica de primer orden y la lógica de enunciados.)

Caso II: Δ es satisfactible en la lógica de enunciados, digamos que con la asignación de verdad v. Entonces usaremos v para dar una estructura $\mathfrak{H}$ en la que Ψ sea satisfactible y $\Gamma \not\models \varphi$, pues $\mathfrak{H}$ nos dará el contraejemplo.

Como en el ejemplo, el universo $|\mathfrak{H}|$ es el universo H de Herbrand, el conjunto de todos los términos del lenguaje de Ψ. Una vez más, los símbolos de función se interpretan de manera autónoma: $f^{\mathfrak{H}}(t_1, \ldots, t_n) = f t_1 \cdots t_n$. Para interpretar el símbolo de predicado P, usamos la asignación de verdad v:

$$\langle t_1, \ldots, t_n \rangle \in P^{\mathfrak{H}} \Longleftrightarrow v(P t_1 \cdots t_n) = V$$

Entonces afirmamos que toda fórmula en Ψ se satisface en $\mathfrak{H}$ por la función identidad $s(x) = x$ sobre las variables. En primer lugar, nótese que $\bar{s}(t) = t$ para todo término t en H; teníamos la misma situación en el paso 4 de la prueba de completud de la sección 5 del capítulo II. En segundo, obsérvese que para una fórmula atómica $P t_1 \cdots t_n$,

$$\models_{\mathfrak{H}} P t_1 \cdots t_n[s] \Longleftrightarrow \langle t_1, \ldots, t_n \rangle \in P^{\mathfrak{H}} \Longleftrightarrow v(P t_1 \cdots t_n) = V.$$

Otra vez por el ejercicio 3 de la sección 4 del capítulo II, toda fórmula δ en Δ se satisface en $\mathfrak{H}$ con s (pues $\bar{v}(\delta) = V$).

Considérese cualquier fórmula en Ψ. Es una fórmula universal; para simplificar la notación, digamos que es $\forall v_1 \forall v_2 \theta(v_1, v_2, v_3)$, donde θ no tiene cuantificadores. Necesitamos verificar, para cualesquiera términos t_1 y t_2 en H, que $\models_{\mathfrak{H}} \theta[[t_1, t_2, v_3]]$.

Esto equivale (por el lema de sustitución) a decir que la fórmula $\theta(t_1, t_2, v_3)$ se satisface en $\mathfrak{H}$ por s. Pero esta fórmula es una instancia de $\forall v_1 \forall v_2\ \theta(v_1, v_2, v_3)$, así que $\theta(t_1, t_2, v_3)$ está en Δ. Como ya se señaló, nuestra construcción se hizo de modo que toda fórmula en Δ se satisficiera en $\mathfrak{H}$ con s. Esto es lo que necesitábamos.

Podemos resumir este resultado de la siguiente manera. Por simplicidad, se establece sólo para enunciados.

Teorema de Herbrand Considérese un conjunto $\Gamma; \varphi$ de enunciados de un lenguaje de primer orden sin igualdad. Sea Δ como se estableció antes. Entonces, o bien (caso I) Δ es insatisfactible en la lógica de enunciados y $\Gamma \models \varphi$, o bien (caso II) Δ es satisfactible en la lógica de enunciados y la estructura $\mathfrak{H}$ construida antes es un modelo de Γ en el que φ es falsa.

(El trabajo de Herbrand formaba parte de su tesis doctoral, que terminó en 1930 poco antes de morir en un accidente de montañismo. La formulación que él hizo de este teorema es bastante distinta de la que aquí presentamos, pero las ideas se desprenden de su trabajo y del de Thoralf Skolem de 1928.)

En el caso I, gracias al teorema de compacidad de la lógica de enunciados, hay un subconjunto finito de Δ que es insatisfactible. Este resultado se puede utilizar para hacer una demostración alternativa del teorema de compacidad para la lógica de primer orden, que no se basa en la sección 5 ni en el cálculo deductivo de la sección 4, ambas del capítulo II.

Además, a partir del enfoque de Herbrand se puede obtener una demostración del teorema de numerabilidad, también independiente de las secciones 4 y 5 del capítulo II. Consideremos el caso especial en el que $\Gamma = \emptyset$. Si φ es válida, entonces, conforme se generen más y más elementos de Δ, llegaremos a un punto en el que tendremos un conjunto insatisfactible, algo que se puede reconocer usando tablas de verdad. Si φ no es válida, entonces, a medida que generemos más y más elementos de Δ, estaremos construyendo una estructura en la cual φ falla, pero dicha estructura es infinita y la construcción nunca termina.

Ejercicios

1. Demuestre la siguiente versión mejorada del teorema de Löwenheim-Skolem: Sea $\mathfrak{A}$ una estructura para un lenguaje numerable. Sea S un subconjunto numerable de $|\mathfrak{A}|$. Entonces hay una *subestructura* numerable $\mathfrak{B}$ de $\mathfrak{A}$, con $S \subseteq |\mathfrak{B}|$, tal que para toda función s de las variables en $|\mathfrak{B}|$ y toda fórmula de primer orden φ,

$$\models_{\mathfrak{A}} \varphi[s] \quad \text{sii} \quad \models_{\mathfrak{B}} \varphi[s].$$

   Sugerencia: Seleccione funciones de Skolem para todas las fórmulas. Cierre S bajo las funciones. *Observación*: Una subestructura $\mathfrak{B}$ con esta propiedad se conoce como una subestructura *elemental*. Nótese que esta propiedad implica (tomando φ como un enunciado) que $\mathfrak{A} \equiv \mathfrak{B}$. Por un lado, esta forma nos permite concluir algo más fuerte que lo que afirmamos en la sección 6 del capítulo II, ya que no sólo obtenemos que $\text{Th}\,\mathfrak{A}$ tiene *algún* modelo numerable, sino que en particular obtenemos un *sub*modelo numerable. Por otro lado, hay que mencionar también que la demostración hace uso del axioma de elección.

2. Generalice el ejercicio anterior al caso no numerable. Suponga que $\mathfrak{A}$ es una estructura para un lenguaje de cardinalidad λ. Sea S un subconjunto de $|\mathfrak{A}|$ con cardinalidad κ. Muestre que hay una subestructura elemental $\mathfrak{B}$ de $\mathfrak{A}$ de cardinalidad a lo más $\kappa + \lambda$ con $S \subseteq |\mathfrak{B}|$.

3. Muestre que el corolario 42B es óptimo en el siguiente sentido:
   (a) Dado cualquier enunciado σ de tipo $\exists_1$, podemos decidir efectivamente si σ es satisfactible o no.
   (b) Dado cualquier enunciado σ de tipo $\forall_1$, podemos decidir efectivamente si σ es válido o no.

4. (a) Postule los dos corolarios (análogos al 42A y al 42B) descritos al final de esta sección.
   (b) Demuestre (a).

5. Repita el ejemplo dado para las expansiones de Herbrand, pero para el inverso: $\exists y\, \forall x\, Pxy \models \forall x\, \exists y\, Pxy$.

Muestre que, en este caso, el conjunto Δ es insatisfactible en la lógica de enunciados.

6. Aplique el método de las expansiones de Herbrand para establecer lo siguiente: $\models \exists x(Px \rightarrow \forall x\, Px)$.

7. Modifique la construcción de la expansión de Herbrand para adecuarla a un lenguaje que incluya la igualdad. *Sugerencia*: En efecto, debe agregarse el paso 5 de la demostración de completud expuesta en la sección 5 del capítulo II. Agregue suficientes enunciados universales para asegurarse de que $\{\langle t_1, t_2\rangle \mid v(t_1 = t_2) = V\}$ es una relación de congruencia.

3. *Lógica multivariada*

Ahora regresamos a los lenguajes de primer orden, pero con muchos tipos de variables, que abarcan diferentes universos. (En la siguiente sección aplicaremos esto al caso en el cual un tipo de variables es para los elementos de un universo, otro para los subconjuntos de ese universo, otro más para las relaciones binarias, y así sucesivamente.)

En matemáticas a veces decimos cosas no muy formales, como "Usamos letras griegas para ordinales, letras mayúsculas para conjuntos de enteros, . . ." En efecto, vamos adoptando distintos tipos de variables (o lenguaje *multivariado*), de modo que cada tipo tiene su propio universo. Ahora nos encargaremos de examinar esta situación de un modo preciso. Como podría esperarse, nada difiere drásticamente del caso usual de un solo tipo de variable (o lenguaje *monovariado*). Ninguno de los resultados de esta sección es muy profundo, y la mayoría de las demostraciones se omiten.

Supongamos que tenemos un conjunto no vacío I, cuyos elementos se denominan tipos de variables, y símbolos dados del siguiente modo:

A. *Símbolos lógicos*

0. Paréntesis: (,).
1. Símbolos de conectivo: $\neg$, $\rightarrow$.

2. Variables: para cada tipo i, hay variables $v_1^i, v_2^i, \ldots$ de tipo i.
3. Símbolos de igualdad: para algunos $i \in I$ puede haber un símbolo $=_i$, que es un símbolo de predicado de tipo $\langle i, i \rangle$.

B. *Parámetros*

0. Símbolos de cuantificador: para cada tipo i hay un símbolo de cuantificador universal $\forall_i$.
1. Símbolos de predicado: para cada $n > 0$ y cada n-ada $\langle i_1, \ldots, i_n \rangle$ de tipos, hay un conjunto (que podría ser vacío) de símbolos de predicado de n argumentos, cada uno de los cuales se dice que es de tipo $\langle i_1, \ldots, i_n \rangle$.
2. Símbolos de constante: para cada tipo i, hay un conjunto (que podría ser vacío) de símbolos de constante, cada uno de los cuales se dice que es de tipo i.
3. Símbolos de función: para cada $n > 0$ y para cada $(n + 1)$-ada $\langle i_1, \ldots, i_n, i_{n+1} \rangle$ de tipos, hay un conjunto (que podría ser vacío) de símbolos de función de n argumentos, cada uno de los cuales se dice que es de tipo $\langle i_1, \ldots, i_n, i_{n+1} \rangle$.

Como se suele hacer, debemos suponer que estas clases de símbolos son disjuntas y además que ningún símbolo es una sucesión finita de otros símbolos.

A cada término se le asignará un único tipo. Definimos el conjunto de los términos de tipo i inductivamente, en forma simultánea para todo i:

1. Cualquier variable de tipo i o símbolo de constante de tipo i es un término de tipo i.

2. Si $t_1, \ldots, t_n$ son términos de tipo $i_1, \ldots, i_n$, respectivamente, y f es un símbolo de función de tipo $\langle i_1, \ldots, i_n, i_{n+1} \rangle$, entonces $ft_1 \cdots t_n$ es un término de tipo i_{n+1}.

Esta definición se puede reformular de un modo que resulte más familiar. El conjunto de los pares $\langle t, i \rangle$ tal que t es un término de tipo i se construye (o se genera) a partir del conjunto básico

$$\{\langle v_n^i, i\rangle \mid n \geq 1 \text{ e } i \in I\} \cup \{\langle c, i\rangle \mid c \text{ es un símbolo de constante de tipo } i\}$$

por medio de las operaciones que, para un símbolo de función de tipo $\langle i_1, \ldots, i_n, i_{n+1}\rangle$, produce el par $\langle ft_1 \cdots t_n, i_{n+1}\rangle$ a partir de los pares $\langle t_1, i_1\rangle, \ldots, \langle t_n, i_n\rangle$.

Una fórmula atómica es una sucesión $Pt_1 \cdots t_n$ que consiste en un símbolo de predicado de tipo $\langle i_1, \ldots, i_n\rangle$ y términos $t_1, \ldots, t_n$ de tipo $i_1, \ldots, i_n$, respectivamente. Las fórmulas no atómicas se forman, entonces, usando los conectivos $\neg$, $\rightarrow$ y los cuantificadores $\forall_i v_n^i$.

Una estructura multivariada $\mathfrak{A}$ es una función sobre el conjunto de los parámetros que asigna a cada uno el tipo correcto de objeto:

1. Al símbolo de cuantificador $\forall_i$, $\mathfrak{A}$ le asigna un conjunto no vacío $|\mathfrak{A}|_i$ llamado el *universo* de $\mathfrak{A}$ de tipo i.

2. A cada símbolo de predicado P de tipo $\langle i_1, \ldots, i_n\rangle$, $\mathfrak{A}$ le asigna una relación

$$P^{\mathfrak{A}} \subseteq |\mathfrak{A}|_{i_1} \times \cdots \times |\mathfrak{A}|_{i_n}.$$

3. A cada símbolo de constante c de tipo i, $\mathfrak{A}$ le asigna un punto $c^{\mathfrak{A}}$ en $|\mathfrak{A}|_i$.

4. A cada símbolo de función f de tipo $\langle i_1, \ldots, i_n, i_{n+1}\rangle$, $\mathfrak{A}$ le asigna una función

$$f^{\mathfrak{A}} : |\mathfrak{A}|_{i_1} \times \cdots \times |\mathfrak{A}|_{i_n} \rightarrow |\mathfrak{A}|_{i_n+1}.$$

Las definiciones de verdad y de satisfacción son las obvias, dado que $\forall_i$ se ha interpretado como "para todos los elementos del universo $|\mathfrak{A}|_i$ de tipo i".

En una estructura multivariada, los universos de los varios tipos pueden o no ser disjuntos; pero ya que no tenemos símbolos de igualdad *entre* tipos, cualquier situación de universos no disjuntos debe considerarse accidental. En particular, siempre habrá una estructura elementalmente equivalente cuyos universos son disjuntos.

Reducción a la lógica monovariada

A veces los lenguajes multivariados pueden ser convenientes (como veremos en la siguiente sección); pero no hay nada esen-

cial que se pueda hacer con ellos que no se pueda hacer también sin ellos. En seguida plantearemos esta afirmación de un modo más preciso.

Consideraremos un lenguaje monovariado que tiene todos los símbolos de predicado, de constante y de función de nuestro lenguaje multivariado supuesto. Además, tendrá un símbolo de predicado Q_i de un argumento para cada i en I. Hay una traducción sintáctica que convierte cada fórmula multivariada φ en una fórmula monovariada φ^*. En esta traducción, todos los símbolos de igualdad se reemplazan por $=$. El único otro cambio está en los cuantificadores (el símbolo de cuantificador y las variables cuantificadas): reemplazamos

$$\forall_i v_n^i __ v_n^i __$$

por

$$\forall v\,(Q_i v \rightarrow __ v __),$$

donde v es una variable elegida de modo que no haya conflicto con las otras variables. Entonces los cuantificadores de tipo i están "relativizados" a Q_i. (Las variables libres se dejan sin cambio.)

Volviendo a la semántica, podemos transformar una estructura multivariada $\mathfrak{A}$ en una estructura $\mathfrak{A}^*$ para el lenguaje monovariado anterior. El universo $|\mathfrak{A}^*|$ es la unión $\bigcup_{i\in I}|\mathfrak{A}|_i$ de todos los universos de $\mathfrak{A}$. Le asignamos a Q_i el conjunto $|\mathfrak{A}|_i$. La estructura $\mathfrak{A}^*$ concuerda con $\mathfrak{A}$ en todos los símbolos de predicado y de constante. Para cada símbolo de función f, la función $f^{\mathfrak{A}^*}$ es una extensión arbitraria de $f^{\mathfrak{A}}$. (Desde luego, este último enunciado no especifica $f^{\mathfrak{A}^*}$ por completo. Los resultados que daremos para $\mathfrak{A}^*$ se cumplen para cualquier estructura obtenida del modo que acabamos de describir.)

Lema 43A Un enunciado multivariado σ es verdadero en $\mathfrak{A}$ sii σ^* es verdadero en $\mathfrak{A}^*$.

Para probar esto, afirmamos algo más fuerte acerca de las fórmulas:

$$\models_{\mathfrak{A}} \varphi[s] \iff \models_{\mathfrak{A}^*} \varphi^*[s],$$

donde $s\,(v_n^i) \in |\mathfrak{A}|_i$. Esta afirmación se prueba por inducción.

Consideremos ahora la otra dirección. Una estructura monovariada no siempre se puede convertir en una estructura multivariada. Por lo tanto, impondremos algunas condiciones. Sea Φ el conjunto que consta de los siguientes enunciados monovariados:

1. $\exists v\, Q_i\, v$, para cada i en I.
2. $\forall v_1 \cdots \forall v_n\, (Q_{i_1} v_1 \to \cdots \to Q_{i_n} v_n \to Q_{i_{n+1}} f v_1 \cdots v_n)$, para cada símbolo de función f de tipo $\langle i_1, \ldots, i_n, i_{n+1}\rangle$. Incluimos el caso $n = 0$, en el cual el enunciado anterior se convierte en $Q_i c$ para un símbolo de constante c de tipo i.

Nótese que la estructura anterior $\mathfrak{A}^*$ es un modelo de Φ. Un modelo monovariado $\mathfrak{B}$ de Φ se puede convertir en un modelo multivariado $\mathfrak{B}^\natural$. La conversión se lleva a cabo del modo natural:

$|\mathfrak{B}^\natural|_i = Q_i^{\mathfrak{B}}$;

$P^{\mathfrak{B}^\natural} = P^{\mathfrak{B}} \cap (Q_{i_1}^{\mathfrak{B}} \times \cdots \times Q_{i_n}^{\mathfrak{B}})$, donde P es un símbolo de predicado de tipo $\langle i_1, \ldots, i_n\rangle$;

$c^{\mathfrak{B}^\natural} = c^{\mathfrak{B}}$;

$f^{\mathfrak{B}^\natural} = f^{\mathfrak{B}} \cap (Q_{i_1}^{\mathfrak{B}} \times \cdots \times Q_{i_n}^{\mathfrak{B}} \times Q_{i_{n+1}}^{\mathfrak{B}})$, la restricción de $f^{\mathfrak{B}}$ a $Q_{i_1}^{\mathfrak{B}} \times \cdots \times Q_{i_n}^{\mathfrak{B}}$, donde f es un símbolo de función de tipo $\langle i_1, \ldots, i_n, i_{n+1}\rangle$.

Lema 43B Si $\mathfrak{B}$ es un modelo de Φ, entonces $\mathfrak{B}^\natural$ es una estructura multivariada. Además, un enunciado multivariado σ es verdadero en $\mathfrak{B}^\natural$ sii σ^* es verdadero en $\mathfrak{B}$.

La prueba es similar a la del lema 43A.

Nótese que en general $\mathfrak{B}^{\natural *}$ no es igual a $\mathfrak{B}$. (Por ejemplo, $|\mathfrak{B}|$ puede contener puntos que no pertenecen a ningún $Q_i^{\mathfrak{B}}$.) Por otro lado, $\mathfrak{A}^{*\natural}$ sí es igual a $\mathfrak{A}$.

Teorema 43C En el lenguaje multivariado

$$\Sigma \models \sigma$$

sii en el lenguaje monovariado

$$\Sigma^* \cup \Phi \models \sigma^*.$$

Demostración ($\Rightarrow$) Supongamos que $\Sigma \models \sigma$ y sea $\mathfrak{B}$ un modelo monovariado de $\Sigma^* \cup \Phi$ (donde $\Sigma^* = \{\sigma^* \mid \sigma \in \Sigma\}$). Entonces, por el lema 43B, $\mathfrak{B}^\natural$ es un modelo de Σ. Por lo tanto, $\mathfrak{B}^\natural$ es un modelo de σ. Así que, nuevamente por el lema 43B, $\mathfrak{B}$ es modelo de σ^*.

($\Leftarrow$) En forma similar, con el lema 43A. ⊣

Usando el teorema 43C, podemos inferir ahora los siguientes tres teoremas a partir de los resultados correspondientes para la lógica monovariada.

Teorema de compacidad Si todo subconjunto finito de un conjunto Σ de enunciados multivariados tiene un modelo, entonces Σ tiene un modelo.

Demostración Supongamos que todo subconjunto finito Σ_0 de Σ tiene un modelo multivariado $\mathfrak{A}_0$. Entonces cualquier subconjunto finito Σ_0^* de Σ^* tiene un modelo $\mathfrak{A}_0^*$. En consecuencia, por el teorema de compacidad ordinario, Σ^* tiene un modelo $\mathfrak{B}$. Entonces, $\mathfrak{B}^\natural$ es un modelo de Σ. ⊣

Teorema de numerabilidad Para un lenguaje multivariado recursivamente numerado, el conjunto de los números de Gödel de los enunciados lógicamente válidos es recursivamente numerable.

Demostración Para un enunciado multivariado σ, por el teorema 43C,

$$\models \sigma \quad \text{sii} \quad \Phi \models \sigma^*.$$

Como Φ es recursivo, $\mathrm{Cn}\,\Phi$ es recursivamente numerable. Pero σ^* depende recursivamente de σ, así que podemos aplicar el ejercicio 7(b) de la sección 5 del capítulo III. ⊣

Teorema de Löwenheim-Skolem Para cualquier estructura multivariada (de un lenguaje numerable) hay una estructura numerable elementalmente equivalente.

Demostración Supongamos que la estructura dada es $\mathfrak{A}$. Entonces $\mathfrak{A}^*$ es un modelo monovariado de $(\mathrm{Th}\,\mathfrak{A})^* \cup \Phi$.

De ahí que, por el teorema de Löwenheim-Skolem ordinario, $(\mathrm{Th}\,\mathfrak{A})^* \cup \Phi$ tiene un modelo numerable $\mathfrak{B}$. En consecuencia, $\mathfrak{B}^\natural$ es un modelo de $\mathrm{Th}\,\mathfrak{A}$ y es elementalmente equivalente a $\mathfrak{A}$. ⊣

4. *Estructuras generales*

Regresamos ahora a la discusión sobre la lógica de segundo orden que empezamos en la sección 1 de este capítulo. Ahí discutimos (a) la sintaxis, es decir, el conjunto de fórmulas de segundo orden, y (b) la semántica, es decir, el concepto de estructura (que fue el mismo que para las de primer orden) y la definición de satisfacción y de verdad.

En esta sección pretendemos dejar (a) sin cambios, pero queremos presentar una alternativa para (b). La idea se puede plantear muy brevemente: ahora consideraremos el lenguaje (que previamente concebimos como un lenguaje de segundo orden) como un lenguaje elemental (es decir, de primer orden) con varios tipos de variables. El resultado será dejar abierto a la interpretación no sólo el universo que abarcan las variables individuales, sino también los universos para las variables de predicado y de función. En particular, este enfoque es adecuado para la teoría de números, caso que examinaremos brevemente al final de esta sección.

El lenguaje multivariado

A pesar de que en última instancia queremos considerar la gramática de la sección 1 de este capítulo, será conveniente considerar un lenguaje multivariado (de primer orden) construido a partir del lenguaje de segundo orden de esa misma sección. Tomamos $\aleph_0$ tipos: el tipo individual (con variables $v_1, v_2, \ldots$); para cada $n > 0$, el tipo de predicado de n argumentos (con variables $X_1^n, X_2^n, \ldots$); y para cada $n > 0$, el tipo de función de n argumentos (con variables $F_1^n, F_2^n, \ldots$). Usaremos la igualdad $(=)$ sólo entre términos de tipo individual. Los parámetros de predicado y de función de nuestro lenguaje de segundo orden dado también serán parámetros del lenguaje multivariado, y tomarán, como argumentos, términos del tipo individual. (Para un parámetro de función f, el término $f\vec{t}$ es de tipo individual;

los únicos términos de tipo de predicado o de función son las variables de esos tipos.)

Además, usaremos ahora dos clases nuevas de parámetros. Para cada $n > 0$, hay un parámetro de predicado de *pertenencia* ε_n que toma, como argumentos, un término del tipo de predicado n-ario (es decir, una variable X_m^n) y n términos de tipo individual. Por ejemplo:

$$\varepsilon_3 X^3 \, v_2 v_1 v_8$$

es una fórmula. Su interpretación propuesta es que la terna denotada con $\langle v_2, v_1, v_8 \rangle$ debe pertenecer a la relación denotada con X^3. Ésta es exactamente la interpretación asignada previamente a la fórmula de segundo orden

$$X^3 \, v_2 v_1 v_8,$$

y de hecho aconsejamos al lector que identifique mentalmente la cercanía de estas dos fórmulas.

Para cada $n > 0$, hay también un parámetro de función *evaluación* E_n, que toma como argumentos un término del tipo de función n-aria (es decir, una variable F_m^n) y n términos de tipo individual. El término resultante,

$$E_n F^n \, t_1 \cdots t_n,$$

es él mismo de tipo individual. Nuevamente aconsejamos al lector que identifique la cercanía del término $E_n F^n t_1 \cdots t_n$ con el anterior $F^n t_1 \cdots t_n$.

Hay un modo obvio de traducir entre el lenguaje de segundo orden de la sección 1 de este capítulo y el presente lenguaje multivariado. En una dirección agregamos los símbolos ε_n y E_n; en la otra los quitamos. El propósito de estos símbolos es hacer que el lenguaje esté de acuerdo con la sección 3 de este capítulo.

Una estructura multivariada tiene universos para cada tipo y asigna objetos adecuados a los diversos parámetros (como se describió en la sección anterior). Para empezar, queremos probar que, sin pérdida de generalidad, podemos suponer que ε_n se interpreta como pertenencia genuina y E_n como evaluación genuina.

Teorema 44A Sea $\mathfrak{A}$ una estructura para el lenguaje multivariado descrito, tal que los diferentes universos de $\mathfrak{A}$ son disjuntos. Entonces existe un homomorfismo h de $\mathfrak{A}$ sobre una estructura $\mathfrak{B}$ tal que:

(a) h es uno a uno, de hecho, es la identidad, sobre el universo de los individuos (de lo cual se sigue que

$$\models_{\mathfrak{A}} \varphi[s] \quad \text{sii} \quad \models_{\mathfrak{B}} \varphi[h \circ s]$$

para cada fórmula φ).

(b) El universo de predicados n-arios de $\mathfrak{B}$ consiste de ciertas relaciones n-arias sobre el universo de individuos, y $\langle R, a_1, \ldots, a_n \rangle$ está en $\varepsilon_n^{\mathfrak{B}}$ sii $\langle a_1, \ldots, a_n \rangle \in R$.

(c) El universo de funciones n-arias de $\mathfrak{B}$ consiste de ciertas funciones n-arias sobre el universo de individuos, y $E_n^{\mathfrak{B}}(f, a_1, \ldots, a_n) = f(a_1, \ldots, a_n)$.

Demostración Como los universos de $\mathfrak{A}$ son disjuntos, podemos definir h sobre cada universo por separado. Sobre el universo de los individuos U, h es la identidad; sobre el universo de tipo de predicados de n argumentos,

$$h(Q) = \{ \langle a_1, \ldots, a_n \rangle \mid \text{cada } a_i \text{ está en } U \text{ y } \langle Q, a_1, \ldots, a_n \rangle \text{ está en } \varepsilon_n^{\mathfrak{A}} \}.$$

Entonces

$$\langle a_1, \ldots, a_n \rangle \in h(Q) \quad \text{sii} \quad \langle Q, a_1, \ldots, a_n \rangle \text{ está en } \varepsilon_n^{\mathfrak{A}}. \qquad (1)$$

De modo similar, sobre el universo de tipo de funciones de n argumentos,

$h(g)$ es la función n-aria sobre U cuyo valor en $\langle a_1, \ldots, a_n \rangle$ es $E_n^{\mathfrak{A}}(g, a_1, \ldots, a_n)$.

Entonces

$$h(g)(a_1, \ldots, a_n) = E_n^{\mathfrak{A}}(g, a_1, \ldots, a_n). \qquad (2)$$

Para $\varepsilon_n^{\mathfrak{B}}$ tomamos simplemente la relación de pertenencia,

$$\langle R, a_1, \ldots, a_n \rangle \text{ está en } \varepsilon_n^{\mathfrak{B}} \quad \text{sii} \quad \langle a_1, \ldots, a_n \rangle \in R. \qquad (3)$$

Para $E_n^{\mathfrak{B}}$ tomamos la función evaluación,

$$E_n^{\mathfrak{B}}(f, a_1, \ldots, a_n) = f(a_1, \ldots, a_n). \tag{4}$$

En los otros parámetros (heredados del lenguaje de segundo orden), $\mathfrak{B}$ coincide con $\mathfrak{A}$.

Entonces está claro que h es un homomorfismo de $\mathfrak{A}$ sobre $\mathfrak{B}$. Que h preserva ε_n se sigue de (1) y (3), donde en (3) tomamos $R = h(Q)$. Asimismo, de (2) y (4) se sigue que h preserva E_n.

Finalmente, tenemos que verificar la afirmación entre paréntesis de la parte (a). Esto se sigue de la versión multivariada del teorema de homomorfismo de la sección 2 del capítulo II, usando el hecho de que tenemos igualdad sólo para el tipo de los individuos, donde h es uno a uno. ⊣

Por el teorema anterior, podemos restringir la atención a las estructuras $\mathfrak{B}$, donde ε_n y E_n están dadas por (b) y (c) del teorema. Pero como $\varepsilon_n^{\mathfrak{B}}$ y $E_n^{\mathfrak{B}}$ están determinadas por el resto de $\mathfrak{B}$, en realidad no las necesitamos. Cuando las eliminamos, tenemos una preestructura general para nuestra gramática de segundo orden.

Estructuras generales para lenguajes de segundo orden

Estas estructuras proporcionan la semántica alternativa mencionada al principio de esta sección.

Definición Una *preestructura general* $\mathfrak{A}$ para nuestro lenguaje de segundo orden consiste en una estructura (en el sentido original) junto con los conjuntos adicionales siguientes:

(a) para cada $n > 0$, un *universo de relaciones* n-arias, que es un conjunto de relaciones n-arias sobre $|\mathfrak{A}|$;

(b) para cada $n > 0$, un *universo de funciones* n-arias, que es un conjunto de funciones de $|\mathfrak{A}|^n$ en $|\mathfrak{A}|$.

$\mathfrak{A}$ es una *estructura general* si, además, todos los enunciados de comprehensión son verdaderos en $\mathfrak{A}$.

La última oración de la definición requiere una explicación. Primero, un enunciado de comprehensión es un enunciado que se obtiene como generalización de una fórmula de comprehensión (véase el ejemplo 3 de la sección 1 de este capítulo). Por lo tanto, es una generalización de

$$\exists \mathbf{X}^n \forall v_1 \cdots \forall v_n (\mathbf{X}^n v_1 \cdots v_n \leftrightarrow \varphi),$$

donde $\mathbf{X}^n$ no aparece libre en φ, o bien una generalización de

$$\forall v_1 \cdots \forall v_n \exists ! v_{n+1} \psi \rightarrow \\ \exists \mathbf{F}^n \forall v_1 \cdots \forall v_{n+1} (\mathbf{F}^n v_1 \cdots v_n = v_{n+1} \leftrightarrow \psi),$$

donde $\mathbf{F}^n$ no aparece libre en ψ. (Aquí φ y ψ pueden tener variables individuales, variables de predicado y variables de función.)

En seguida debemos aclarar qué significa que un enunciado de comprehensión (o, más bien, cualquier enunciado de segundo orden) sea verdadero en $\mathfrak{A}$. Supongamos, pues, que $\mathfrak{A}$ es una preestructura general. Entonces, un enunciado σ es verdadero en $\mathfrak{A}$ sii el resultado de transformar σ en un enunciado multivariado (agregando ε_n y E_n) es verdadero en $\mathfrak{A}$, con ε_n interpretada como pertenencia y E_n como evaluación.

Más en general, sea φ una fórmula de segundo orden, y sea s una función que asigna a cada variable individual un elemento de $|\mathfrak{A}|$, a cada variable de predicado un elemento del universo de relaciones de $\mathfrak{A}$, y a cada variable de función un elemento del universo de funciones de $\mathfrak{A}$. Entonces decimos que $\mathfrak{A}$ satisface φ con s (lo cual se escribe $\models^{G}_{\mathfrak{A}} \varphi[s]$) sii la versión multivariada de φ se satisface con s en la estructura $\mathfrak{A}$, donde ε_n se interpreta como pertenencia y E_n como evaluación.

Las consecuencias esenciales de esta definición de satisfacción son las siguientes, que podrían compararse con 5 y 6 de la página 107.

$\models^{G}_{\mathfrak{A}} \forall \mathbf{X}^n \varphi[s]$	sii para toda R en el universo de las relaciones n-arias de $\mathfrak{A}$, $\models^{G}_{\mathfrak{A}} \varphi[s(\mathbf{X}^n \mid R)]$.
$\models^{G}_{\mathfrak{A}} \forall \mathbf{F}^n \varphi[s]$	sii para toda f en el universo de las funciones n-arias de $\mathfrak{A}$, $\models^{G}_{\mathfrak{A}} \varphi[s(\mathbf{F}^n \mid f)]$.

Éste es entonces el enfoque alternativo mencionado al inicio de esta sección; esto implica tratar la gramática de segundo orden como una gramática multivariada de primer orden disfrazada. Como este enfoque es básicamente de primer orden, tenemos el teorema de Löwenheim-Skolem, el teorema de compacidad y el teorema de numerabilidad.

Teorema de Löwenheim-Skolem Si el conjunto Σ de enunciados en un lenguaje numerable de segundo orden tiene un modelo general, entonces tiene un modelo general numerable.

Aquí un modelo general numerable es aquel en el que todo universo es numerable (o de manera equivalente, que la unión de todos los universos es numerable).

Demostración Sea Γ el conjunto de los enunciados de comprehensión. Entonces $\Sigma \cup \Gamma$, visto como conjunto de enunciados multivariados, tiene un modelo multivariado numerable por el teorema de Löwenheim-Skolem de la sección anterior. Por el teorema 44A, existe una imagen homeomórfica de ese modelo que es una preestructura general que satisface $\Sigma \cup \Gamma$, y por lo tanto es un modelo general de Σ. ⊣

Teorema de compacidad Si todo subconjunto finito de un conjunto Σ de enunciados de segundo orden tiene un modelo general, entonces Σ tiene un modelo general.

Demostración La prueba es exactamente como la anterior. Todo subconjunto finito de $\Sigma \cup \Gamma$ tiene un modelo multivariado, de modo que podemos aplicar el teorema de compacidad de la sección anterior. ⊣

Teorema de numerabilidad Supongamos que el lenguaje es recursivamente numerado. Entonces, el conjunto de los números de Gödel de los enunciados de segundo orden que son verdaderos en toda estructura general es recursivamente numerable.

Demostración Un enunciado σ es verdadero en toda estructura general sii σ es consecuencia, como enunciado multivariado, de Γ. Y sabemos que $\sharp\Gamma$ es recursivo. ⊣

Los dos teoremas anteriores aseguran que existe un cálculo deductivo aceptable tal que τ es deducible a partir de Σ sii τ es verdadero en todo modelo general de Σ (véanse las observaciones al principio de la sección 4 del capítulo II). Pero ahora que sabemos que existe tal cálculo deductivo completo, no hay razón para desarrollarlo detalladamente.

Podemos comparar los dos enfoques de la semántica de segundo orden como sigue: la versión de la sección 1 de este capítulo (a la que llamaremos lógica *absoluta* de segundo orden) es una criatura híbrida, en la cual el significado de los parámetros se deja abierto a la interpretación por estructuras; sin embargo, la interpretación de ser (por ejemplo) un subconjunto no se deja abierta, sino que se trata con un significado fijo. La versión de la presente sección (lógica *general* de segundo orden) evita apelar a una noción fija de subconjunto y es, en consecuencia, reducible a la lógica de primer orden. En ese aspecto se asemeja a la teoría axiomática de conjuntos, donde se habla de conjuntos y de conjuntos de conjuntos, y así sucesivamente, pero la teoría es una teoría de primer orden.

Al agrandar la clase de las estructuras, la lógica general de segundo orden disminuye los casos en que se cumple la implicación lógica. Es decir, si todo modelo general de Σ es modelo general de σ, entonces se sigue que $\Sigma \models \sigma$ en la lógica absoluta de segundo orden. Pero el inverso es falso. Por ejemplo, tomemos $\Sigma = \emptyset$: El conjunto de los enunciados verdaderos en todos los modelos generales es un subconjunto recursivamente numerable del conjunto no aritmético de los enunciados válidos de la lógica absoluta de segundo orden.

Modelos del análisis

Podemos ilustrar la idea de esta sección dirigiendo la atención al caso particular más interesante: los modelos generales de la teoría de los números de segundo orden. Consideremos, pues, el lenguaje de segundo orden para la teoría de los números, con los parámetros **0**, **S**, $<$, $\cdot$ y **E**. Tomamos como nuestro conjunto de axiomas el conjunto A_E^2 obtenido a partir de A_E agregando como duodécimo elemento el postulado de inducción de Peano (ejemplo 2, sección 1 de este capítulo). Del ejercicio 1 de la sección 1, también de este capítulo, podemos concluir

que cualquier modelo (en la semántica de esa sección) de A_E^2 es isomorfo a $\mathfrak{N}$.

Pero ¿qué podemos decir de los modelos *generales* de nuestro conjunto de axiomas? Pueden diferir de $\mathfrak{N}$ en cualquiera de dos maneras (o en ambas). Como antes, podemos usar el teorema de compacidad para construir modelos generales (no estándar) de los axiomas que tienen números infinitos (es decir, modelos $\mathfrak{A}$ con un elemento mayor que el denotado por $\mathbf{S}^n\mathbf{0}$ en el orden $<^{\mathfrak{A}}$). También podemos encontrar modelos generales (no absolutos) en los cuales, por ejemplo, el universo de los conjuntos (el universo de las relaciones unarias) es menor que todo el conjunto potencia del universo de individuos. De hecho, cualquier modelo general numerable debe ser de esta clase.

Es tradicional entre los lógicos referirse a la teoría de los números de segundo orden como ***análisis***. El nombre se debe a que es posible identificar a los números reales con los conjuntos de los números naturales. En la teoría de los números de segundo orden tenemos cuantificadores sobre los conjuntos de los números naturales que pueden verse como cuantificadores sobre los números reales. Aunque puede cuestionarse lo adecuado del nombre, su uso está bien establecido. Por un *modelo del análisis* entenderemos un modelo general del conjunto anterior de axiomas A_E^2.

Definimos un *ω-modelo del análisis* como un modelo del análisis en el que el universo de los individuos es $\mathbb{N}$ y $\mathbf{0}$ y $\mathbf{S}$ denotan a los 0 y S estándar. (Como consecuencia, $<$, $+$, $\cdot$ y $\mathbf{E}$ también tienen denotaciones estándar.) La motivación para estudiar los ω-modelos se puede explicar como sigue: tenemos una comprensión clara —o así lo creemos— del conjunto $\mathbb{N}$; pero de su conjunto potencia $\mathcal{P}\,\mathbb{N}$ no podemos decir lo mismo. Por ejemplo, no sabemos si su cardinalidad es $\aleph_1$ o $\aleph_2$ o más. Así que es razonable dejar fijo aquello de lo que estamos seguros ($\mathbb{N}$), pero dejar abierto a interpretación por una estructura aquello de lo que no estamos seguros ($\mathcal{P}\,\mathbb{N}$).

Entre los ω-modelos del análisis hay un modelo *absoluto*, cuyo universo de relaciones n-arias consta de todas las relaciones n-arias sobre $\mathbb{N}$ (y cuyos universos de funciones constan de todas las funciones posibles). Un enunciado de primer orden es

verdadero en un ω-modelo arbitrario del análisis sii es verdadero en $\mathfrak{N}$. Pero tal vez el ω-modelo no coincida con el modelo absoluto en los enunciados de segundo orden.

En el siguiente teorema afirmamos que un ω-modelo del análisis está completamente determinado por su universo de conjuntos (es decir, por su universo de relaciones unarias).

Teorema 44B Si $\mathfrak{A}$ y $\mathfrak{B}$ son ω-modelos del análisis que tienen los mismos universos de relaciones unarias, entonces $\mathfrak{A} = \mathfrak{B}$.

Demostración Supongamos que R pertenece al universo de las relaciones de tres argumentos de $\mathfrak{A}$. Sea $\langle R \rangle$ la "compresión" de R a una relación unaria:

$$\langle R \rangle = \{\langle a,b,c \rangle \mid \langle a,b,c \rangle \in R\}.$$

Nuestra función codificadora de sucesiones es recursiva y, por lo tanto, definible en teoría de los números de primer orden por una fórmula φ. $\langle R \rangle$ está en el universo de conjuntos de $\mathfrak{A}$ en virtud del enunciado de comprehensión

$$\forall X^3 \exists X^1 \forall u [X^1 u \leftrightarrow \exists v_1 \exists v_2 \exists v_3 (\varphi(v_1, v_2, v_3, u) \wedge X^3 v_1 v_2 v_3)].$$

Entonces $\langle R \rangle$ está en el universo de conjuntos de $\mathfrak{B}$: lo decodificamos por medio de un argumento similar. R está en el universo de relaciones de tres argumentos de $\mathfrak{B}$ en virtud del enunciado de comprehensión

$$\forall X^1 \exists X^3 \forall v_1 \forall v_2 \forall v_3 [X^3 v_1 v_2 v_3 \leftrightarrow \exists u (\varphi(v_1, v_2, v_3, u) \wedge X^1 u)].$$

Un argumento similar se aplica a los universos de funciones. ⊣

En consecuencia, podemos identificar un ω-modelo del análisis con su universo de conjuntos (que está incluido en $\mathcal{P}\mathbb{N}$). No toda subclase de $\mathcal{P}\mathbb{N}$ es, entonces, un ω-modelo del análisis, sino sólo aquellos para los cuales se satisfacen los enunciados de comprehensión.

EJEMPLOS DE ω-MODELOS Sólo necesitamos especificar el universo de conjuntos.

1. $\mathcal{P}\mathbb{N}$ es el modelo absoluto.

2. Sea $(A; \in_A)$ un modelo de los axiomas más comunes de la teoría de conjuntos tal que (i) la relación $\in_A$ es la relación de pertenencia $\{\langle a,b\rangle \mid a \in A,\ b \in A \text{ y } a \in b\}$ sobre el universo A, y (ii) A es transitivo, es decir, si $a \in b \in A$, entonces $a \in A$. Por lo tanto, la colección de todos los subconjuntos de $\mathbb{N}$ que pertenecen a A es un ω-modelo del análisis.

3. Para una clase $\mathcal{A} \subseteq \mathcal{P}\mathbb{N}$, definimos $\mathbb{D}\mathcal{A}$ como la clase de todos los conjuntos $B \subseteq \mathbb{N}$ que son definibles en la ω-preestructura con universo de conjuntos $\mathcal{A}$ por una fórmula del lenguaje de la teoría de números de segundo orden, aumentado con parámetros para cada conjunto de $\mathcal{A}$. Entonces definimos por recursión transfinita sobre los ordinales:

$$\begin{aligned} \mathcal{A}_0 &= \emptyset, \\ \mathcal{A}_{\alpha+1} &= \mathbb{D}\mathcal{A}_\alpha, \\ \mathcal{A}_\lambda &= \textstyle\bigcup_{\alpha<\lambda} \mathcal{A}_\alpha \quad \text{para } \lambda \text{ límite.} \end{aligned}$$

Por consideraciones de cardinalidad vemos que esto deja de crecer en algún ordinal β para el cual $\mathcal{A}_{\beta+1} = \mathcal{A}_\beta$. Sea β_0 el mínimo β tal; se puede demostrar (a partir del teorema de Löwenheim-Skolem) que β_0 es un ordinal numerable. $\mathcal{A}_{\beta_0}$ coincide con $\bigcup_\alpha \mathcal{A}_\alpha$ (unión sobre todos los ordinales α) y se llama la clase de los *conjuntos analíticos ramificados*. Es un ω-modelo del análisis; la verdad de los enunciados de comprehensión se sigue del hecho de que $\mathbb{D}\mathcal{A}_{\beta_0} \subseteq \mathcal{A}_{\beta_0}$.

SUGERENCIAS PARA LECTURAS ADICIONALES

Barwise, Jon (comp.), *Handbook of Mathematical Logic*, North-Holland, Amsterdam, 1978. Este "manual" recopila 31 artículos que exponen la teoría de modelos, la teoría de conjuntos, la teoría de la recursión y la teoría de la demostración, escritos por expertos.

Barwise, Jon y John Etchemendy, *The Language of First-Order Logic*, Center for the Study of Language and Information, Stanford, 1992. Éste es un libro de texto introductorio e incluye un disco para el paquete de software *Tarski's World*. Los mismos autores han elaborado los paquetes de software *Turing's World* y *Hyperproof*.

Bell, J.L. y M. Machover, *A Course in Mathematical Logic*, North-Holland, Amsterdam, 1977.

Boolos, George y Richard Jeffrey, *Computability and Logic*, 3a. ed., Cambridge University Press, Cambridge, 1989 (1974). Este libro de texto, dirigido a un público diferente, aborda de manera sólida algunos de los temas del presente texto.

Chang, C.C. y H.J. Keisler, *Model Theory*, 3a. ed., North-Holland, Amsterdam, 1990 (1973). Este texto sigue siendo el libro clásico de teoría de modelos.

Enderton, Herbert B., *Elements of Set Theory*, Academic Press, Nueva York, 1977. Éste es el libro favorito del autor sobre teoría de conjuntos.

Hodges, Wilfrid, *A Shorter Model Theory*, Cambridge University Press, Cambridge, 1997. Ésta es una versión abreviada de su libro *Model Theory*, publicado en 1993.

Rogers, Hartley, *Theory of Recursive Functions and Efective Computability*, McGraw-Hill, Nueva York, 1967. Este libro es todavía la obra clásica en su campo.

Shoenfield, Joseph R., *Mathematical Logic*, Association for Symbolic Logic y A.K. Peters, Natick, Mass., 2000. Publicado originalmente

por Addison-Wesley en 1967, ofrece un tratamiento más sintético, para estudiantes de posgrado.

Van Heijenoort, Jean (comp.), *From Frege to Gödel: A Source Book in Mathematical Logic, 1879–1931,* Harvard University Press, Cambridge, Mass., 1967. Recopila 46 artículos fundamentales en lógica, traducidos al inglés y con comentarios.

LISTA DE SÍMBOLOS

Los números indican la página donde aparece por primera vez el símbolo.

$\dashv$	13	$\langle x_1, \ldots, x_n \rangle$	16	V	38
$\Rightarrow$	13	$A \times B$	17	$\bar{v}$	39
$\Leftarrow$	13	dom 17	4	$\models$	42–43
$\Leftrightarrow$	13	ran R	17–18	$\models\!\dashv$	43
$\therefore$	13	cam R	18	$\mathcal{D}$	55
$\not\models$	13	A^n	18	C^*	59
$\in$	13	$F : A \to B$	18	C_*	59
$\notin$	13	$f \circ g$	18, 261	$\bar{h}$	63
$=$	13	$\mathbb{R}$	19	$\#$	73
$A;t$	14	$[x]$	19	B^n_α	74–75
$\emptyset$	14	$A \sim B$	22	$\perp$	80–81
$\{x_1, \ldots, x_n\}$	14	card A	22	$\top$	80–81
$\{x \mid _x_\}$	14	$\preceq$	23	$\downarrow$	81–82
$\mathbb{N}$	14	$\aleph_0$	24	$\mid$	81–82
$\mathbb{Z}$	14	$\neg$	27	$+$	81–82
$\subseteq$	15	$\to$	27	$*$	96
$\mathcal{P}$	15	$\wedge$	27	$\forall$	104
$\cup$	15	$\vee$	28	$\exists$	105, 118
$\cap$	15	$\leftrightarrow$	30	v_n	105
$\bigcup$	15	$\mathcal{E}$	34	$=$	105
$\bigcap$	15	F	38	$<$	108, 265

ÍNDICE ANALÍTICO

ÍNDICE

Una introducción matemática a la lógica se terminó de imprimir en septiembre de 2004 en los talleres de Formación Gráfica, S.A. de C.V. (Matamoros 112, Col. Raúl Romero, C.P. 57630, Cd. Nezahualcóyotl, Edo. de México). Para su composición y formación, realizadas por computadora, se utilizaron el programa LaTeX 2_ε y tipos New Baskerville.
El tiraje consta de 1000 ejemplares.